# HP StorageWorks

# Edge Switch Element Manager user guide

FW 07.00.00/HAFM SW 08.06.00

Part number: AA–RS2HD–TE
Fourth edition: March 2005

**Legal and notice information**



Printed in the US.

# Edge Switch Element Manager user guide

# Contents

## Figures

## Tables

# About this guide

This guide provides information that lets you:

- Configure and manage the Edge Switch 2/24 and Edge Switch 2/32
- Access logs and maintenance information using the Element Manager
- Install and manage optional features
- Contact technical support

## Intended audience

This book is intended for use by system administrators who are experienced with the following:

- Fibre Channel technology
- StorageWorks Fibre Channel switches by Hewlett-Packard

## Related documentation

For a list of corresponding documentation included with this product, refer to the Related Documents section of the *HP StorageWorks Edge Switch release notes*.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks web site:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Industry Association web site, http://www.fibrechannel.org.

These and other HP documents can be found on the HP documents web site: http://www.docs.hp.com.

# Document conventions and symbols

**Table 1** Document conventions

| Convention | Element |
|---|---|
| Medium blue text: Figure 1 | Cross-reference links and e-mail addresses |
| Medium blue, underlined text (http://www.hp.com) | Web site addresses |
| **Bold font** | • Key names<br>• Text typed into a GUI element, such as into a box<br>• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes |
| *Italics font* | Text emphasis |
| `Monospace font` | • File and directory names<br>• System output<br>• Code<br>• Text typed at the command-line |
| *`Monospace, italic font`* | • Code variables<br>• Command-line variables |
| **`Monospace, bold font`** | Emphasis of file and directory names, system output, code, and text typed at the command line |

⚠ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

**IMPORTANT:** Provides clarifying information or specific instructions.

**NOTE:** Provides additional information.

**TIP:** Provides helpful hints and shortcuts.

# Rack stability

**WARNING!** To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, secure racks together.
- Extend only one rack component at a time. Racks may become unstable if more than one component is extended.

# HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

## HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-345-1518.
- Elsewhere, visit the HP web site: http://www.hp.com. Then click **Contact HP** to find locations and telephone numbers.

## Helpful web sites

For third-party product information, see the following HP web sites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com

# 1 Element Manager overview

This chapter is an introduction to the Element Manager that is used to manage the HP StorageWorks Edge Switch 2/24 and Edge Switch 2/32. It is intended as a quick reference for features available through the main Element Manager window of the High Availability Fabric Manager (HAFM) application.

# Managing the edge switch

You can manage an edge switch through several different interfaces. These interfaces are as follows:

- The Element Manager and HAFM

  Installed on HAFM appliance shipped from the factory or supplied by the customer. (You access the Element Manager through the HAFM *application*.)
- Embedded Web Server (EWS)

  Using a browser-capable PC with an Internet connection to the switch, you can monitor and manage the switch through the EWS interface embedded in the switch firmware. The interface provides a GUI similar to the Element Manager and supports switch configuration, statistics monitoring, and basic operation.

  To launch the EWS interface:

1. Enter the director's IP address as the Internet Uniform Resource Locator (URL) into any standard browser.
2. Enter a user name and password at the login screen. The browser then becomes a management console. (Refer to the Embedded Web Server interface online help or the *HP StorageWorks Embedded Web Server user guide* for details on use.)

---

**NOTE:** The default user name for the right to view status and other information is "operator." The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is "Administrator." The default password for both user names is "password."

---

- Command Line Interface (CLI).

  The CLI allows you to access many HAFM application and Element Manager functions while entering commands during a Telnet session with the switch. The primary purpose of the CLI is to automate management of many switches using scripts. The CLI is not an interactive interface; no checking is done for pre-existing conditions, and no prompts display to guide users through tasks. Refer to the *HP StorageWorks CLI reference guide for Directors and Edge Switches* for more information.
- Simple Network Management Protocol (SNMP).

  An SNMP agent is implemented through the Element Manager. It allows administrators on SNMP management workstations to access product management information using any standard network management tool. Administrators can assign Internet Protocol (IP) addresses and corresponding community names for up to six workstations functioning as SNMP trap message recipients. Refer to the *HP StorageWorks SNMP reference guide for Directors and Edge Switches* for more information.

This manual provides details on the Element Manager for the Edge Switch 2/24 and Edge Switch 2/32 only. This manual does not cover the Embedded Web Server (EWS) interface.

# Element manager description

The Element Manager for Edge Switch products is a Java-based graphical user interface (GUI) that provides in-depth management, configuration, and monitoring functions for individual switches and their field-replaceable
units (FRUs).

The Element Manager provides graphical views of switch hardware components and displays of component status. By positioning the mouse pointer on icons, graphics, panels, and other visual elements in these views and clicking the left or right mouse button, you can quickly manage and monitor switches on your network.

The server software for the HAFM and Element Manager comes installed on the HAFM appliance.

You can install the HAFM and Element Manager clients on remote computer systems, as shown Figure 1 on page 17. For instructions, refer to the section in *HP StorageWorks HA-Fabric Manager user guide* that pertains to the operating system of your computer.

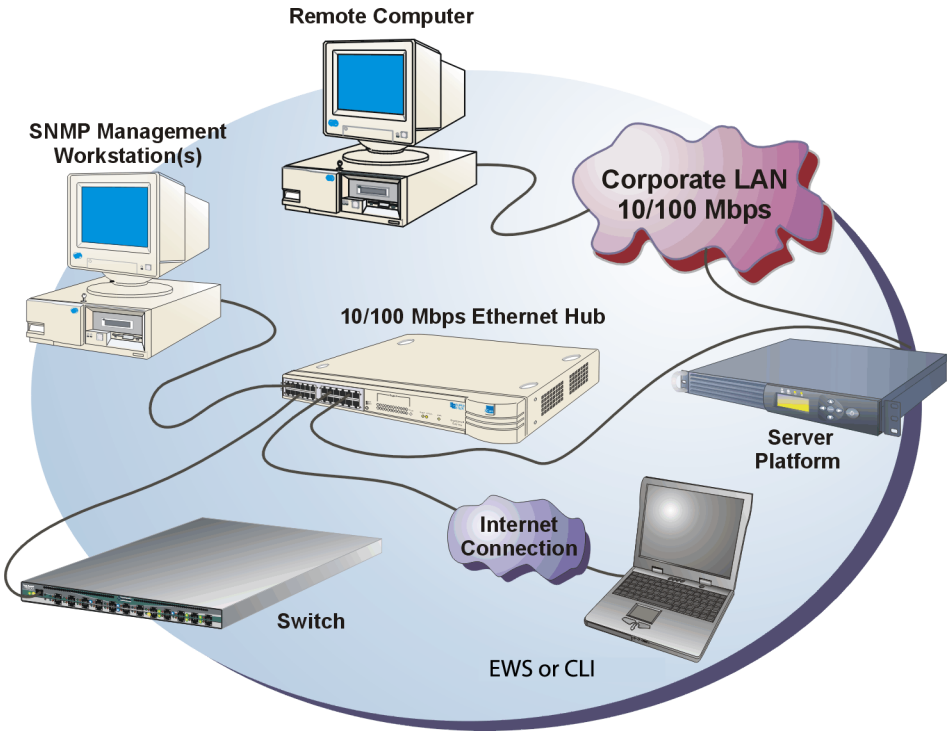



**Figure 1** HAFM appliance and remote client configuration (dual Ethernet)

Using the Element Manager, you can:

- Back up and restore configuration data.
- Clear the system error indicator.
- Configure Fibre Channel operating parameters for the fabric, such as R_A_TOV, E_D_TOV, switch priority, and interop mode. You can also configure Fibre Channel operating parameters for the switch, such as preferred and insistent domain ID, rerouting delay, and domain RSCNs.
- Configure individual ports with a port name describing the node attached to the port.
- Configure keys for new features.
- Configure interoperability mode for open switch fabrics.
- Configure Preferred Paths for interswitch links (ISLs).
- Configure link incident (LIN) alerts.
- Configure a nickname to display instead of the world wide name (WWN) for the switch and attached nodes.
- Configure Port Binding and port speed.
- Configure SNMP trap recipients and community names.
- Configure Switch Binding if the optional SANtegrity Binding feature is installed.
- Configure Open Trunking if the optional Open Trunking feature is installed.
- Configure Open Systems Management Server features if the optional Open Systems Management Server feature is installed.
- Configure the switch name, location, description, and contact person.
- Control individual Fibre Channel ports by blocking/unblocking operation, enabling LIN alerts and Port Binding, and running internal and external loopback diagnostics.
- Display field replaceable unit (FRU) properties such as the FRU name, physical position in the switch (chassis slot number), active/failed state, part number, and serial number.
- Display information for individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.
- Display information on nodes attached to ports.
- Display port performance and statistics.
- Display vital product data for the switch, such as the system name, description, contact person, location, status, model number, firmware and Engineering Change (EC) level, and manufacturer.
- Enable beaconing for ports and the switch unit.
- Enable Alternate Control Prohibited (ACP) to restrict access to FICON switch connectivity parameters.
- Monitor the operational status of the switch and each of its hardware field-replaceable units.
- Perform an initial program load (IPL).
- Perform maintenance tasks for the switch, including maintaining firmware levels, administering the Call Home Notification feature, accessing the switch logs, and collecting data to support failure analysis.
- Reset port operation.

- Run port diagnostics.
- Set the date and time on the switch.

**NOTE:** You may perform configuration for some features through both the HAFM and the Element Manager. You must also enable Element Manager feature permissions for Administrative, Operator, and Maintenance user levels through the HAFM. When this guide refers to the HAFM for specific tasks, you should see the HAFM online help or the *HP StorageWorks HA-Fabric Manager user guide* for detailed instructions.

# Using the Element Manager

This section provides a general overview of the Element Manager and its functions. For details on performing specific tasks and using specific dialog boxes, see the appropriate chapters in this manual.

## Using dialog boxes

Buttons such as **OK**, **Activate**, **Close**, and **Cancel** initiate functions in a dialog box. Generally, these buttons have the following functions:

- **OK** saves the entered information and closes the dialog box.
- **Activate** saves the entered information or activates the indicated changes.
- **Close** closes the dialog box and saves the data you entered.
- **Cancel** cancels the operation and closes the dialog box without saving the information you entered.

## Keyboard navigation

Use standard keyboard navigation in dialog boxes. For example, use the **Tab**, arrow, and backspace keys to move through dialog box fields, and **Enter** to perform default button functions.

## Illustrations used in this guide

Figures containing HAFM and Element Manager screens in this manual are included for illustration purposes only. These illustrations may not match exactly what you see through your server or workstation. Title bars have been removed from the illustrations, and fields in the illustrations may contain different data than in screens displayed on your system.

Additionally, some illustrations display the Edge Switch 2/24 and some display the Edge Switch 2/32. There a number of differences between the Edge Switch 2/24 and Edge Switch 2/32. For example, the Edge Switch 2/24 uses an FL_Port and the Edge Switch 2/32 does not. These differences are reflected in the screen shots.

# Opening the Element Manager

To open the Element Manager:

- In HAFM, double-click the appropriate edge switch product icon in the Physical/Topology Map, as shown in Figure 2. The Element Manager window displays, showing the default Hardware View. See Figure 3

Or,

- Right-click the appropriate edge switch product icon in the Physical/Topology Map, as shown in Figure 2. A pop-up menu displays.


**Figure 2** edge switch icon

Click **Element Manager**. The Element Manager window displays, showing the default Hardware View. See Figure 3.

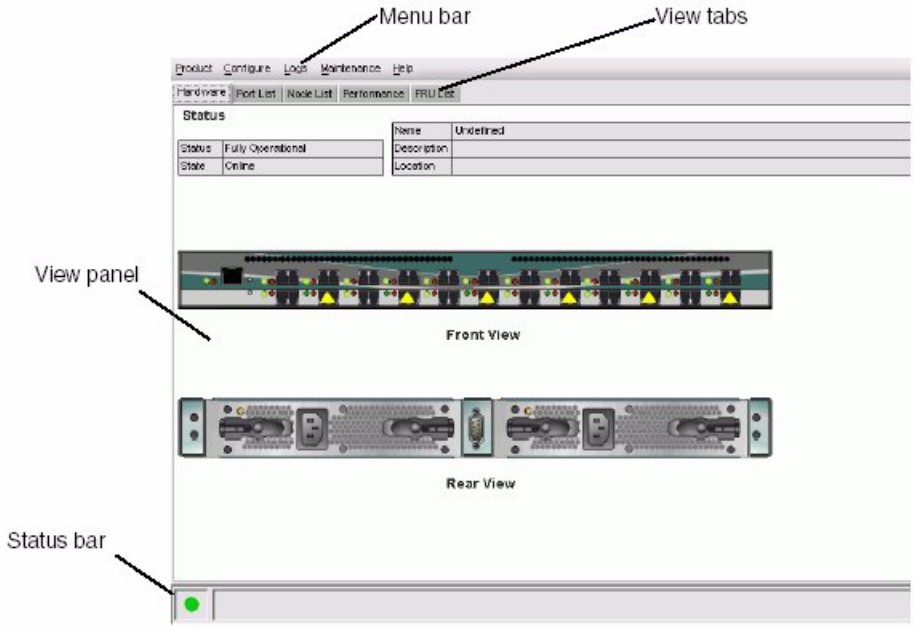



**Figure 3** Element Manager window (Hardware View for the Edge Switch 2/24)

The user manuals and other documentation are provided in Portable Document Format (PDF) and are available in *<Install_Home>\docs*.

**NOTE:** The HAFM window is still available as a separate window. You can drag the Element Manager window away from the other window and view both windows on your desktop, or you can minimize one or both of them to icons, if desired. You can have a maximum of four Element Manager windows open concurrently.

## Opening the Online Help

Use the following steps to open the online help:

1. Open the Element Manager for the switch from the HAFM desktop, as described in "Opening the Element Manager" on page 20.
2. Select **Help > Contents** or press **F1**.

## Window layout and function

The main Element Manager window is divided into four main areas, as shown in Figure 3 on page 20: Menu bar, View tabs, View panel, and Status bar. You can use the features in these areas to configure switch operation, monitor performance, and access maintenance features.

### Menu bar

The menu bar on the Element Manager window contains the following menus:

- Product
- Configure Logs
- Maintenance
- Help

Click on the name of a menu to display a list of menu options. Select an option to open a dialog box that allows you to perform configuration and maintenance tasks and to view logs.

If a menu option contains a check box, click in the box to add a check mark and enable a function. Click a check box containing a check mark to remove the check mark and disable the function.

#### Product menu

Click one of the following options on the **Product** menu:

**Management style**

This option is available on the Edge Switch 2/32 only. It includes options:

- **Open Systems**—The management style that is used for open fabrics. Open Systems is the default management style.
- **FICON**—The management style that is most useful when attaching to IBM S/390 Enterprise Servers.

**Port**

This option provides a secondary port menu only when the Hardware View, Port List View, or Performance View displays in the View panel. To use this menu for a specific port, click a port in the Hardware View, a port's row in the Port List View, or a port's bar graph in the Performance View. The menu contains options which are identical to those that display when you right-click the port, port row, or port bar graph in those views. For detail on these options, see "Port menu" on page 57.

**FRU**

Click a power supply module/fan in the Hardware View only and select **Product > FRU > FRU Properties** to display the FRU properties dialog box. The FRU Properties dialog box can also be displayed when you double-click the FRU in the Hardware View. For details on these options, see "FRU List View" on page 71.

**Clear system error Light**

Select this option to turn off the amber system error LED, located below the green/blue power LED on the switch front bezel.

**Enable unit beaconing**

Click the check box for this option to toggle unit beaconing on or off. When the check box has a check mark, unit beaconing is on, and the amber system error light on the switch front bezel blinks to help users locate the actual unit in an equipment room. When you click the check box to remove the check mark, unit beaconing is disabled and the amber LED goes out. You can only enable beaconing if there are no system errors (the system error light is off).

**Properties**

Select this option to display the Switch Properties dialog box. This dialog box contains the switch name, description, location, and contact person configured through the Configure Identification dialog box. Also included is other product information, as detailed in "Displaying switch information" on page 54. You can also display this dialog box by double-clicking an area on the illustration in the Hardware View, away from a hardware component.

**Close**

Select this option to close the Element Manager window.

## Configure menu

Select **Configure** on the menu bar to display a menu that lists the following options. For detailed information on using these options, see "Configuring the switch" on page 77.

**Identification**

Select this option to display the Configure Identification dialog box. Enter the following information in this dialog box:

- **Name**—Enter a product name. Note that you can set this name as the nickname for the switch's WWN, using the **Set Name as Nickname** check box. The nickname then displays instead of the WWN in Element Manager views.

**NOTE:** You can configure a maximum of 2,048 nicknames.

- **Description**—Enter a unique product description.
- **Location**—Enter the product's location.
- **Contact**—Enter a contact either by name, phone number, or e-mail address.

**NOTE:** This information displays in the identification table at the top of the Hardware View and in the HAFM **P**hysical/Topology Map, if the view is configured to display names.

### Operating parameters

This option lets you configure switch and fabric parameters, as follows:

- Select **Switch Parameters** to display the Configure Switch Parameters dialog box, which allows you to set Fibre Channel operating parameters. Using this dialog box, you can set parameters, such as preferred domain ID (1 through 31), Domain RSCNs, and Suppress RSCNs on Zone Set Activations. In addition, you can also enable the rerouting delay feature. See "Configuring operating parameters" on page 79 for more information.
- Select **Fabric Parameters** to display the Configure Fabric Parameters dialog box, which allows you to set parameters for fabric operation. In this dialog box, you can set the resource allocation time-out value (R_A_TOV) and error detect time-out value (E_D_TOV) in tenth-of-a-second increments. You can also set other fabric operating parameters, such as switch priority level (**Principal**, **Default**, or **Never Principal**) and interop mode. You must take the switch offline through the Set Online State dialog box to configure these parameters. See "Configuring fabric parameters" on page 81 for more information.

### Preferred path

Select this option to configure an ISL between switches and directors. The ISL consists of the source port of the switch being configured, the exit port of the same switch, and the domain ID of the destination switch. Each switch must be configured for its part of the desired path for optimal performance. You may need to configure Preferred Paths for all switches along the desired path for proper multi-hop Preferred Path operation. For more details about this feature, see "Configuring a Preferred Path" on page 144.

### Switch binding

This submenu provides two options if the SANtegrity Binding feature is installed through the Configure Feature Key dialog box: **Change State** and **Edit Membership List**. Clicking **Change State** displays the Switch Binding State Change dialog box, which you use to activate Switch Binding according to a specific connection policy (Restrict E_Ports, Restrict F_Ports, or Restrict All Ports). **Edit Membership List** allows you to create a list of switches and devices that you want to allow exclusively to attach to switch ports. For more information, see "Configuring a feature key" on page 104 and "Switch binding" on page 153.

**Ports**

Select this option to display the Configure Ports dialog box. For each port you can provide a name, block or unblock operation, enable LIN alerts, enable Fabric Address Notification (FAN), define a type (G, F, E, Gx, and Fx), configure Port Binding, define port speed, and enable Port Binding.

**NOTE:** Ports are automatically configured as G_Ports if no device is connected, F_Ports if a device is connected, E_Ports if a switch is connected, and FL_Port if connected to a loop device.

**SNMP agent**

Select this option to display the Configure SNMP dialog box. Use this dialog box to configure network addresses and community names for up to six SNMP trap recipients. You can also authorize write permissions to enable SNMP management stations to modify writable Management Information Base (MIB) variables. In addition, you can enable authorization traps to be sent to management stations when unauthorized stations request access to switch SNMP data.

**Management server**

Edge Switch 2/32 only. Select this option to display the Configure Open Systems Management Server dialog box. This dialog box will only display if the Open Systems Management Server feature is enabled for the switch. (This feature allows you to manage switches without using the HAFM *application*.) Use this menu option to configure an open systems inband management program to function with the switch.

**NOTE:** To use these procedures, you must have enabled the Open Systems Management Server through the Configure Feature Key dialog box. See "Configuring a feature key" on page 104 for more information.

**Features**

Select this option to display the Configure Feature Key dialog box. Use this dialog box to enter a feature key to enable optional features that you have purchased for the switch. See "Configuring a feature key" on page 104 for more information.

**Date and time**

Select this option to display the Configure Date and Time dialog box. Use this dialog box to set the current date and time in the switch. When the **Periodic Date/Time Synchronization** check box is checked, the **Date and Time** fields are grayed out (disabled), and the switch date and time are periodically synchronized with the HAFM appliance date and time. If the **Periodic Date/Time Synchronization** check box is not checked, you can set the date and time in the dialog box fields manually.

**Threshold alerts**

Select this option to configure threshold alerts for ports. A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific switch ports or port types (E_Ports F_Ports, or FL_Ports).

Using this option, you can configure:

- A name for the alert.
- A threshold type for the alert (Rx, Tx, or both).
- Active or inactive state of the alert.
- Threshold criteria. This includes configuring the threshold as the percent of port traffic capacity utilized (**% utilization)**. You must also configure the time interval during which the throughput is measured, and the maximum cumulative time that the throughput percentage threshold can be exceeded during this time interval before an alert is generated.

**Open trunking**

Select this option to enable the optional Open Trunking feature. This feature monitors the average data rates of all traffic flows on ISLs (from a receive port to a target domain). It also periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimize bandwidth use. The feature can be installed through the Configure Feature Key dialog box. See "Configuring a feature key" on page 104 and "Open Trunking" on page 158 for more information.

**Export configuration report**

Select this option to display the Export Configuration Report dialog box, which enables you to specify a file name in which to save an American Standard Code for Information Interchange (ASCII) text file containing all current user-definable configuration options in a printable format. Note that this file cannot be read back into the Element Manager in order to set configuration parameters.

**Enable Web Server**

Select this option to enable the Embedded Web Server (EWS) on the switch. This puts a check mark in the box next to the menu option. Click the option again to clear the check mark and disable the EWS interface. When this option is disabled, users at remote workstations cannot access the EWS interface.

**Enable Telnet**

Select this option to enable telnet access to the switch. This puts a check mark in the box next to the menu option. Click the option again to clear the check mark and disable telnet access. When this option is disabled, users at remote workstations cannot access the switch through telnet to use the Command Line Interface (CLI).

**Enable Alternate Control Prohibited (ACP)**

Select this option to display Alternate Control Prohibited (ACP) in the Configure menu by selecting the check box to set the ACP on or off. When the ACP is checked, alternate control prohibited is on and alternate managers cannot change FICON Switch connectivity parameters. Alternate Control Prohibited checkbox is only visible for switches that support ACP.

## Logs menu

The Element Manager provides logs that show a record of various events that have occurred on the switch. Select the **Logs** menu to display the following options.

For detailed information on using these dialog boxes, see "Using logs" on page 119.

### Audit log

This log provides a record of all configuration changes made on the switch. Each entry displays the date and time of the change, a description of the change, the source of the change (such as the HAFM appliance or SNMP management station), and an identifier for the source, such as the IP address of the HAFM appliance or SNMP management station.

### Event log

Select this option to display the switch event log. This log provides a record of significant events that have occurred on the switch, such as hardware failures, degraded operation, and port problems. Each entry includes the date and time of the event, a reason code for the event, the severity level, a brief description, and up to 32 bytes of supplementary event data. Refer to the appropriate service manual for your Edge Switch for more information.

### Hardware log

This log displays information on FRUs inserted and removed from the switch. Each log entry includes the name of the FRU inserted or removed, the slot position relative to identical FRUs installed, whether the FRU was inserted or removed, the FRU part number and serial number, and the date and time the FRU was inserted or removed.

### Link incident log

The link incident (LIN) log displays the most recent incidents with their date and time, port number, and a description of the incident. A link incident can be one of several conditions detected on a fiber optic link. For a list of events that may cause a link incident to be written to the log, see "Link Incident log" on page 126.

This log includes link incidents from all group configuration elements. Individual link incidents can also be viewed by drilling down to the Element Manager for that group configuration element.

### Threshold alert log

This log provides notifications of threshold alerts. Besides the date and time that the alert occurred, it also displays information that was configured through the **Threshold Alerts** option under the **Configure** menu. This includes the alert name, the port for which the alert is configured, the type of alert (transmit throughput, receive throughput, or both), threshold utilization of traffic capacity, minutes the threshold was configured for, and the configured time interval for the threshold. For more details on this log, see "Threshold alert log" on page 127.

### Open Trunking log

This log provides details on flow rerouting through switch ports. This log displays only if the optional Open Trunking feature is installed. For more details on this log, see "Open Trunking log" on page 161.

### Security log

The Security log includes information about security events. For more details on this log, see "Security log" on page 128.

**Advanced log: Embedded Port log**

This log provides a detailed history log of all traffic passing through the embedded port. For more details on this log, see "Embedded Port log (Advanced log)" on page 129.

**Advanced log: Switch Fabric log**

This log includes information about switches in a fabric. For more details on this log, see "Switch Fabric log (Advanced log)" on page 131.

## Maintenance menu

Select the **Maintenance** menu on the menu bar to display a list of the following options. For detailed information on using these dialog boxes, see "Using maintenance features" on page 133.

**Port(s) Diagnostics**

This option displays the Port(s) Diagnostics dialog box. Use this dialog box to run internal and external loopback tests on ports. Refer to the appropriate service manual for your Edge Switch for instructions.

**Data collection**

This option displays the Save Data Collection dialog box. Use this dialog box to collect maintenance data into a file. This file is used by support personnel to diagnose system problems. Refer to the appropriate service manual for your Edge Switch for instructions.

**IPL**

Select this option to initiate an Initial Program Load on the switch. A dialog box appears to allow you to confirm the IPL. Note that an IPL does not affect any configuration settings done through the Element Manager. This operation does not interrupt port operation.

See the "Executing an IPL" on page 135 for more information.

**Set online state**

Select this option to display the Set Online State dialog box. Use this dialog box to change the online state of the switch to offline or online.

**Firmware library**

Select this option to display the Firmware Library dialog box. This dialog box displays all firmware versions currently installed on the HAFM appliance that can be downloaded to switches. Use this dialog box to add a new firmware version to the HAFM appliance hard disk, modify the description displayed for an existing version, delete a version from the appliance, or download (send) a version for operation on a switch. At most, eight versions of the firmware can be stored in the library.

For additional information on using the firmware library, refer to the following documents:

- *HP StorageWorks Edge Switch 2/24 installation guide* or *HP StorageWorks Edge Switch 2/24 service guide*

or

- *HP StorageWorks Edge Switch 2/32 installation guide* or *HP StorageWorks Edge Switch 2/32 service guide*

**Enable e-mail notification**

The Simple Mail Transfer Protocol (SMTP) server and e-mail recipient addresses are configured in HAFM (not in the Element Manager). E-mail notification is also initially enabled in HAFM for all switches it manages. Note, however, that the **e-mail notification** option on the Element Manager's **Maintenance** menu must be enabled (checked) for e-mail notification to occur for the specific switch.

The default setting for the **Enable e-mail notification** function is enabled (checked). To disable the function, select **Maintenance > Enable e-mail notification** to clear the check box.

For additional information on using this option, see "Enabling e-mail notification" on page 137.

**Enable Call Home notification**

Select **Maintenance > Enable Call Home Notification** to enable the call-home function for the switch. The parameters of the call-home feature are configured in Windows®. Refer to the *HP StorageWorks HA-Fabric Manager Appliance installation guide* for instructions.

For additional information on using this option, see "Enabling or disabling call home notification" on page 138.

**Backup and restore configuration**

Select this option to save the product configuration stored on the switch to the HAFM appliance hard disk or to restore the configuration data from the appliance. Only a single copy of the configuration is kept on the appliance.

This backup is primarily for single-control processor (CTP) systems, where a backup is needed to restore the configuration data to a replacement CTP card. You cannot modify the location or the file name of the saved configuration.

For additional information on using this option, see "Backing up and restoring configuration data" on page 117.

**NOTE:** You can only restore the configuration to a switch with the same IP address.

**Reset configuration**

Select this option to reset all switch configuration data back to the factory defaults. When you choose this option, a confirmation dialog box appears with a warning. For additional information on using this option, see "Resetting configuration" on page 140.

**CAUTION:** This operation resets all configuration data, including any optional features that have been installed. You will need to re-enter your feature key to enable all optional features after resetting the configuration.

## Help menu

Select the **Help** menu on the menu bar to display a list of the following options.

**Contents**

Select this option to display the Help window. The Help window opens with the **Contents** menu visible. You can click the Index pane or click the **Search** icon to conduct a search. The help text provides buttons and hypertext—linked items to help you quickly navigate through information. Use the forward (**>**) and back (**<**) buttons to scroll forward and backward through the displayed help frames. Exit the help feature at any time by clicking the **Close** icon at the top of the Help window.

**About**

Select this option to display the version number for the Element Manager and copyright information.

## View tabs

Select one of the view tabs across the top of the Element Manager window to display the following views in the View panel.

- Hardware
- Port List
- Node List
- Performance
- FRU List

## View panel

Views, selected from the View tabs, display under the tabs in the View panel.

## Hardware View

The Hardware View is the default view that displays in the View panel the first time you open a switch's Element Manager. To return to this view from another view, click the **Hardware** tab. See Figure 4 for an example of this view.

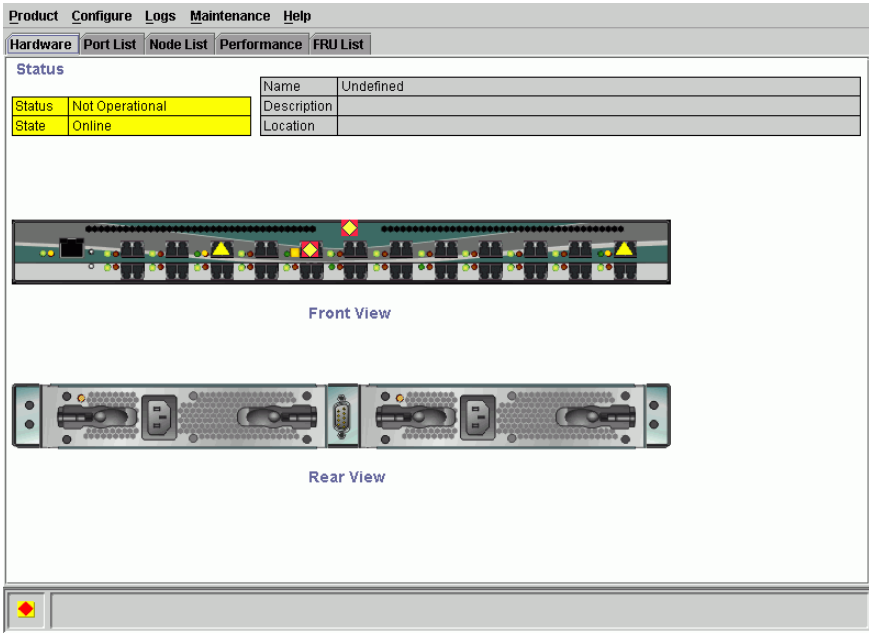



**Figure 4** Hardware View

In the Hardware View, colored indicators reflect the status of actual LEDs on the switch FRUs. The status bar displays a symbol to represent the most degraded status currently reported by any of the switch FRUs. For example, for a port failure, indicated by a blinking red and yellow diamond on a port, a yellow triangle displays on the status bar to indicate a degraded condition. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a red and yellow diamond, which indicates a failure requiring immediate attention.

For an explanation of the different status symbols and the reasons they display in the Hardware View or Port List View, see the table under "Monitoring hardware operation" on page 47.

## Switch menu

Double-click the switch graphic, away from a FRU, to display the Switch Properties dialog box. Right-click a hardware graphic, away from a FRU, to display the following options:

- Properties
- Enable unit beaconing
- Clear system error light
- IPL
- Date and time
- Set online state

For details on menu options, see "Using menu options" on page 55.

For details on navigating and monitoring via the Hardware View, see "Hardware View" on page 46.

### Port menu

Double-click a port to display the Port Properties dialog box. Right-click a port to display the following options:

- Port properties
- Node properties
- Port technology
- Block port
- Enable beaconing
- Port(s) diagnostics
- Clear link incident alerts
- Reset port
- **Port binding**
- Clear threshold alerts

These options are also available when you click a port in the Hardware View and choose the port secondary menu from the **Product** menu on the menu bar.

For details on menu options, see "Port menu" on page 57.

For details on navigating and monitoring via the Hardware View, see "Hardware View" on page 46.

## Port List View

Click the **Port List** view tab. The Port List View appears. This view contains a table of data on all Fibre Channel ports in the switch. This data includes the port number, port name, blocked configuration state, operational state (such as online or failed), type of port, and any alerts. Figure 5 shows an example of the Port List View.

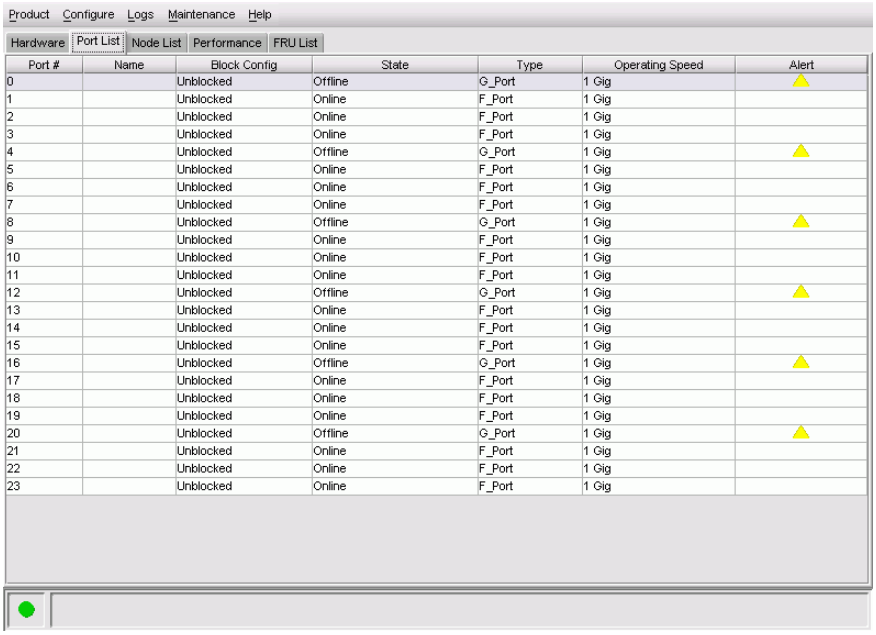



**Figure 5** Port List View

The Port List View displays information about all ports installed in the switch. All data is dynamic and updates automatically. Double-click any row in this view to display the Port Properties dialog box for the port.

Right-click a port row to display the same menu options that display when you right-click a port in the Port Card view or a port's bar graph in the Performance view. These include:

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beaconing**
- **Diagnostics**
- **Channel Wrap** (FICON management style only)
- **Swap Ports** (FICON management style only)
- **Clear Link Incident Alert(s)**
- **Reset Port**

- **Port Binding**
- **Clear Threshold Alert(s)**

These options also display when you click a port row and choose **Product > Port**.These options are also available when you click a port row and then select **Product > Port**.

For details on these menu options, see "Port menu" on page 57.

For details on navigating and monitoring via the Port List View, see "Port List View" on page 61.

## Node List View

Click the **Node List** view tab. The Node List View displays, as show in Figure 6. This view shows a table with information about the node attachments to existing ports, sorted by port number. Information includes the switch port number, port or node addresses, node type, port World Wide Name (WWN), unit type, and BB_Credit.

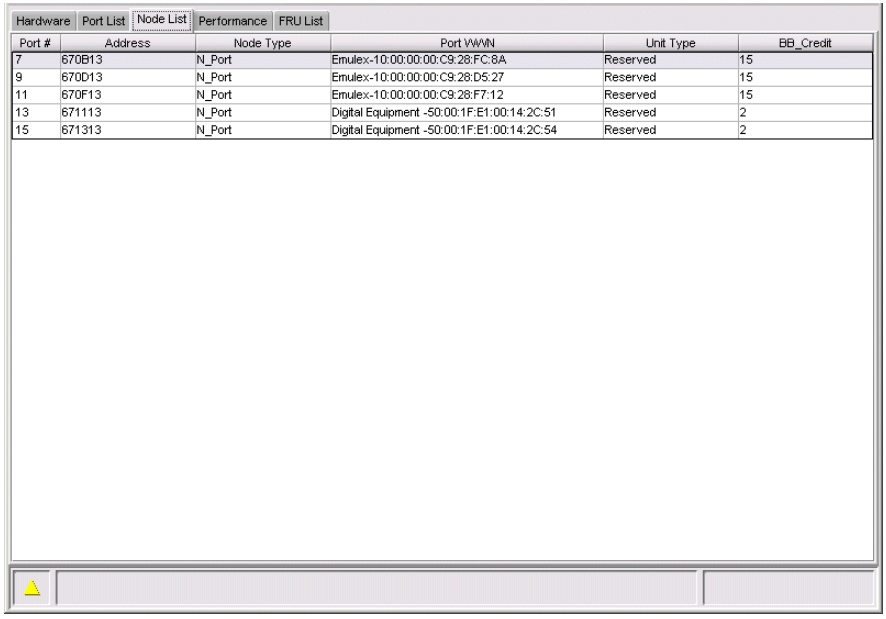



**Figure 6** Node List View

Double-click a port row to highlight it and display the Node Properties dialog box for that port.

Right-click a port row to display the following menu options:

- **Node properties**—Displays the Node Properties dialog box.
- **Port properties**—Displays the Port Properties dialog box.
- **Define nickname**—Displays the Define Nickname dialog box, in which you can define a nickname to display for the attached device instead of the device's 8-byte WWN.

**NOTE:** You can configure a maximum of 2,048 nicknames.

- **Display options**—Allows you to display attached devices listed under the **Port WWN** column in the Node List View by the device's nickname, configured through the **Define Nickname** menu option or the device's WWN.

These options are also available when you click a port row and then select **Product > Port**.

For details on navigating and monitoring via the Node List View, see "Node List View" on page 63.

## Performance View

Click the **Performance** view tab. Figure 7 shows an example of the Performance View. This view provides a graphical display of performance for all ports. The top portion of the Performance View displays bar graphs that show the level of transmit/receive activity for each port. (Use the scroll bar to view bar graphs for all the ports.) The information in this view updates every five seconds.

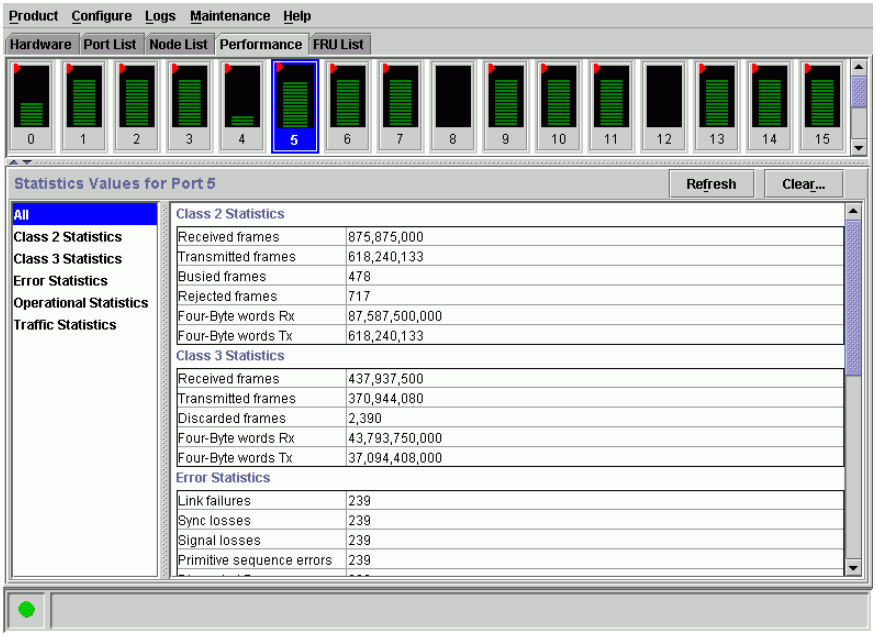



**Figure 7** Performance View (Edge Switch 2/32)

Each bar graph also shows the percentage link utilization for the port. A red arrow marks the highest utilization level reached since the Performance View was opened. If the system detects activity on a port, it represents minimal activity with at least one bar.

When an end device (node) is logged into a port, moving the mouse pointer over the port's bar graph in the Performance View highlights the graph and displays a message with the WWN of the connected node.

If the connected node has more than one port, this is the WWN of the specific port on the node. The following types of messages display:

- `E_Port`—Occurs when a port is functioning as an expansion port (E_Port).
- Port's current online state—Occurs when a port is not logged into an end-device (not functioning as an F_Port) or to another switch (not functioning as an E_Port). This message can also occur when a port is functioning as an FL_Port.
- WWN of the device—Occurs when the port is logged into an end device (functioning as an F_Port).

Right-click a bar graph to display a menu of port-related actions. The options available on this menu are the same as those that are available when you right-click a port in the Hardware View or right-click a row in the Port List View. These include:

- Port properties
- Node properties (Edge Switch 2/32 only)
- Port technology
- Block port
- Enable beaconing
- Port(s) diagnostics
- Clear link incident alert(s)
- Reset port
- Port binding
- Clear threshold alert(s)

**NOTE:** Note that these options are also available when you click a port's graph and then select **Product > Port**.

For details on menu options, see "Port menu" on page 57.

The bottom portion of the Performance View displays cumulative statistical information for the port selected in the bar graph. Values are displayed for cumulative port statistics; error count values for a port, including traffic statistics, Class 2 and 3 accounting statistics; operational statistics; and error statistics. Click a category in the left frame of the statistics area to display only statistics in that category, or click **All** to display values for all categories. Click the **Refresh** button to update the data with current data from the port.

**Clear** clears all of the counters to zero. Clicking this button displays a Clear Port Statistics dialog box. Click the appropriate option button and click **OK** to clear all counters to zero on the selected port only or counters on all ports on the switch.

**NOTE:** Clearing the counters clears the statistics for all users.

For more information about the Performance View, including statistics descriptions, see "Performance View" on page 66.

### FRU List View

To display the FRU List View, click the **FRU List** tab. A table, as shown in Figure 8, displays in the View panel. This table included information about each FRU installed in the switch. All data is dynamic and updates automatically.

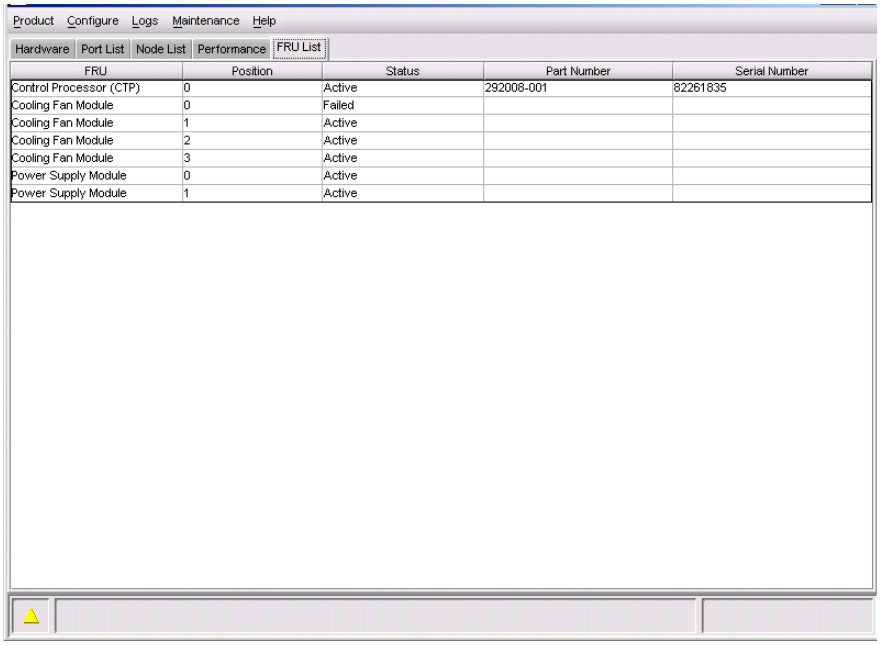



**Figure 8** FRU List View

Double-click a row to display the FRU Properties for the selected FRU.

For details on navigating and monitoring via the FRU List View, see "FRU List View" on page 71.

## Status bar

The status bar is located along the bottom of the Element Manager window. This includes a symbol that displays at the left side of the bar, and messages that display in the panel to the right of the symbol. The symbol indicates the current operating status of the switch, and the messages display to provide more description of menu options as you move the mouse pointer over the options under menu bar menus.

See Table 2 on page 37 for the meaning of these status symbols and of the corresponding alert text that displays in the **edge switch Status** table at the top of the Hardware View in the View panel.

If a gray square displays in the status bar (no Ethernet connection), a reason for the status displays in the **Status** table at the top of the Hardware View. See the **No Link Status** bullet description in "Switch status table" on page 46 for details.

## Switch status symbols

The symbols can appear on the Status Bar:

 –Green Circle

 –Yellow Triangle

 –Red Diamond with Yellow Background

 –Grey Square

Table 2 describes the Status Bar symbols.

**Table 2** Status Bar symbols

| Status Bar | Switch status table text | Description |
|---|---|---|
| Green Circle | Fully Operational | All components and installed ports are operational; no failures. |
| Yellow Triangle | Redundant Failure | A redundant component has failed, such as a power supply, and the backup component has taken over operation. |
| | Minor Failure | A failure occurred which has decreased the switch operational ability. Normal switching operations are not affected. |
| Red Diamond with Yellow Background | NOT OPERATIONAL | A critical failure prevents the switch from performing fundamental switching operations.<br>All fans failed.<br>An installed port failed.<br>Both power supplies failed. |
| Gray Square | Never Connected<br>Link Timeout<br>Protocol Mismatch<br>Duplicate Session<br>Unknown Network Address<br>Incorrect Product Type | Switch status is unknown. This occurs if the Ethernet network connection between the HAFM appliance and the switch cannot be established or if the CTP fails. See the No Link Status bullet description in "Switch status table" on page 46 for details on the status table text. |

## Closing the Element Manager

To close the Element Manager, use the following methods:

- Select **Product > Close**.
- Click the **X** at the top right corner of the Element Manager window.
- Double-click the icon at the top left corner of the Element Manager window, or right-click the icon and click **Close** from the menu that displays.

# Feature keys

Feature keys verify ownership of the Element Manager and optional features that can be purchased for the Element Manager. The feature key, which is encoded with a switch's serial number, can only be configured on the switch or director to which it is assigned.

When you purchase additional Element Manager features, you receive a feature key. The feature keys that you are currently using are included in this key.

Here are some important notes about the Element Manager feature key introduced with this release:

- All edge switches that were purchased prior to the release of firmware 06.00.00 automatically have the Element Manager feature enabled when their firmware is upgraded to version 06.00.00 or later. However, the feature key for the Element Manager is not added or incorporated into the existing feature key.
- Enabling the **Reset Configuration** option through the Element Manager **Maintenance** menu clears all features that were enabled through the Configure Feature Key dialog box. (See "Configuring a feature key" on page 104 for more information.) When you attempt to reinstall features using a feature key assigned for an edge switch prior to the release of 06.00.00, a warning displays that the Element Manager feature key is not installed. You must contact customer support to get a feature key reassigned that includes the Element Manager feature.
- For switches shipped to you with firmware version 06.01.00 or later installed, you must activate the feature keys through the Configure Feature Key dialog box in the Element Manager. See "Configuring a feature key" on page 104 for more information.

## Feature permissions

The system administrator can allow users access to specific functions of Element Manager features through HAFM.

Detailed instructions for assigning permissions are provided in the *HP StorageWorks HA-Fabric Manager user guide*.

There are three permission levels or that can be assigned to specific users:

- Device administration
- Device operation
- Device maintenance
- Security

By default, all users have read-only feature permissions, which allow viewing, but not modifying, data or configurations. You can enable each of the permission levels as either read-only or read/write for specific users.

Users that are assigned a permission level that is required for a specific feature must also be given read/write access to modify any data through the feature. For example, to clear the Audit Log, a user must be assigned Device Administration permission, as well as read/write access. If a user is assigned Device Administration permission, but read-only access, that user can only view the Audit Log.

## Required permissions for Element Manager features

Table 3itemizes specific functions available to Element Manager users who have been assigned Device Administration, Device Operation, and Device Maintenance permissions. Note that the user must also be assigned read/write access to perform functions that modify data or configurations. If a user does not have permission to perform a specific operation, a not-authorized error box appears when the operation is attempted.

**Table 3** Permissions required for feature functions

| Element Manager rights | Device administration | Device operation | Device maintenance | Security administrator |
|---|---|---|---|---|
| Allow or prohibit Matrix, Active (FICON style only) | X | X | | |
| Allow or prohibit Matrix, Stored (FICON style only) | X | X | | |
| Enable Alternative Control Prohibit | X | | | |
| Backup and Restore Configuration | X | X | X | |
| Channel Wrap (FICON management style) (Edge Switch 2/32 only) | X | | X | |
| Clear Audit Log | X | | | |
| Clear Event Log | | | X | |
| Clear Hardware Log | X | | X | |
| Clear LIN Alert | X | X | X | |
| Clear LIN Log | X | | | |
| Clear System Error Light | | | X | |
| Clear Threshold Alerts | X | | | |
| Clear Threshold Event Log | X | | | |

**Table 3** Permissions required for feature functions (continued)

| Element Manager rights | Device administration | Device operation | Device maintenance | Security administrator |
|---|---|---|---|---|
| Configure allow or prohibit Matrix, Active (FICON management style) | X | X | | |
| Configure Addresses – "Active" (FICON management style—Edge Switch 2/32 only) | X | X | | |
| Configure Addresses – "Stored" (FICON management style—Edge Switch 2/32 only) | X | | | |
| Configure Date/Time | X | X | X | |
| Configure Feature Key | X | | | |
| Configure FMS | X | X | | |
| Configure Identification | X | | | |
| Configure Management Server | X | | | |
| Configure Switch Parameters | X | | | |
| Configure Fabric Parameters | X | | | |
| Configure Open Trunking | X | | | |
| Configure Ports: | | | | |
| Blocked | X | X | X | |
| LIN alerts | X | X | | |
| NamE | X | X | | |
| Port binding | X | | | X |
| RX BB_Credit | X | X | | |
| Speed | X | X | | |
| Configure Preferred Path | X | | | |
| Configure SNMP | X | | | |
| Configure Switch Binding: | | | | |
| Connection policy | | | | |
| Enable | X | | | X |
| Membership list | X | | | X |
| | X | | | X |

**Table 3** Permissions required for feature functions (continued)

| Element Manager rights | Device administration | Device operation | Device maintenance | Security administrator |
|---|---|---|---|---|
| Configure Threshold Alerts | X | | | |
| Configure Zoning | X | | | |
| Data Collection | | | X | |
| Date/Time Sync Configuration | X | X | X | |
| Enable Call Home Notification | X | | X | |
| Enable Channel Wrap (FICON Management style) | X | | X | |
| Enable CNT WAN | X | | | |
| Enable Date/Time synchronization | X | X | X | |
| Enable e-mail notification | X | | X | |
| Enable Embedded Web Server | X | | | |
| Enable FRU Beaconing | | | X | |
| Enable Telnet | X | | | |
| Export Configuration | X | X | | |
| IPL | X | X | X | |
| Manage Firmware | | | X | |
| Modify Port Bindings | | | X | |
| Port Diagnostics | | | X | |
| Port Beaconing | X | X | X | |
| Reset Configuration | | | X | |
| Reset Statistics Counters (Performance View) | X | X | | |
| Reset Port | X | | X | |
| SANtegrity Authentication (in Element Manager and Security Center) | X | | | X |
| Set Online State | X | X | X | |

**Table 3** Permissions required for feature functions (continued)

| Element Manager rights | Device administration | Device operation | Device maintenance | Security administrator |
|---|---|---|---|---|
| Swap Ports (FICON management style only) | X | | X | |
| Unit Beaconing | X | X | X | |
| View Event Log | | X | X | |
| View Firmware | | | X | |
| View Hardware Log | X | X | X | |
| View LIN Log | X | X | X | |
| View Open Trunking Log | X | | X | |
| View Security Log | | | | X |
| View SNMP | X | X | X | |
| View Switch Performance Threshold Alert Log | X | X | X | |
| View Threshold Alert Log | X | X | X | |

# Backing up and restoring Element Manager data

You can protect your data by backing it up and then restoring it as necessary.

## What is backed up?

The following data, contained in the `<Install_Home>\Server`, `<Install_Home>\Client`, and `<Install_Home>\Call Home` directories, are backed up to disk:

**NOTE:** `<Install_Home>` refers to the directory where the HAFM application is installed.

- All log files.
- Zoning library (all zone sets and zone definitions). Note that zoning is configured through HAFM.
- Call-home configuration (including phone numbers and dialing options).
- Configuration data.

**NOTE:** This data can also be saved through the **Backup & Restore Configuration** option on the Element Manager **Maintenance** menu.

- Plans. Data is saved if the optional Planning feature is available through HAFM.

- License information.
- User launch scripts.
- User defined sounds.
- All data exported through the **Export** option on the HAFM **SAN** menu.

**NOTE:** Firmware files are NOT backed up.

## Backing Up to a CD

The rack-mount HAFM appliance is backed up to a compact disk, rewritable (CD-RW). As long as a CD-RW disk remains in the CD recorder drive of the HAFM appliance, critical information from both the Element Manager and the HAFM are automatically backed up to the CD-RW disk when the data

directory contents change or when you reboot HAFM.

## Restoring data from a CD

To restore data to HAFM, copy the three folders from the CD-RW (`D:\Backup\`) and paste them in `C:\Program Files\<Install_Home>`. You will be asked if you want to overwrite the existing files; click **Yes**.

## Manual backup procedures

A full data backup occurs the first time that you configure any parameter on a new HAFM appliance.

After this initial backup, a backup only occurs when any data changes or if the HAFM appliance is rebooted. This backup is not a full backup, but only an incremental backup of changed data.

You should do a manual backup to ensure that HAFM data is fully backed up to a CD-ROM disk if any of the following occur:

- You are changing or archiving these disks.
- You have changed a disk and a `Use current disk` message displays.

To manually backup HAFM data:

1. Locate these folders on `C:\<Install_Home>`, where `<Install_Home>` refers to the directory in which the HAFM application is installed:
   - \Server
   - \Client
   - \Call Home

Copy these folders to `X:\backup`. The `X` is the drive letter for your CD-ROM drive where backups occur. Overwrite the existing files.

# 2 Monitoring and managing the switch

This chapter describes how to use the features available in the Element Manager View panel to monitor and manage switch operation. These features include status indicators, menu options, and dialog boxes available through the Hardware View, Port List View, FRU List View, Node List View, and Performance View. This chapter includes the following topics:

# Hardware View

The Hardware View is the default view when you open the Element Manager. If another view displays, you can display the Hardware View by clicking the Hardware view tab on the Element Manager window. Using this graphical view of the switch, you can view status symbols and simulated light emitting diode (LED) indicators. You can also display data and use mouse functions to monitor status and obtain vital product information for the switch and its hardware components.

## Identifying FRUs

Move the mouse pointer over parts of the switch graphic in the Hardware View to display labels identifying each hardware component. The labels also specify each components slot position in the chassis relative to identical components installed in the switch. Components include:

- Power supply module. Note that each AC connector on the rear of the unit is the location of an internal power supply (two total).
- Ports (small form factor LC transceivers).

## Monitoring switch operation

Monitor the operating status of the switch using the switch Status table on the Hardware View and the status indicator on the status bar at the bottom of the Element Manager window.

### Switch status table

The Status table at the top of the Hardware View displays the switch's operational status, operational state, name, description, and location, as follows:

- **Status**—See Table 4 on page 72 for the meaning of the text that displays in the switch **Status** table and the corresponding status symbols that display on the status bar.
- **State**—The **State** field displays one of the following:
  - **Offline**—When the switch is "OFFLINE," all ports are offline. The ports cannot accept a login from an attached device or cannot connect to other switches. You can configure this state through the Set Online State dialog box. See "Setting online state" on page 136 for instructions.
  - **Online**—All unblocked ports are able to connect with devices. You can configure this state through the Set Online State dialog box. See "Setting online state" on page 136 for instructions. Note that the switch automatically goes online after a power-up, an initial machine load (IML), or initial program load (IPL).
  - **Coming online**—This is a transitional state that occurs just before the switch goes online. This state normally only happens briefly, unless there is a problem reaching the online state.
  - **Going offline**—This is a transitional state that occurs just before the switch goes offline. This state normally only happens briefly, unless there is a problem reaching the offline state.
- **No Link Status**—If the Ethernet network connection between the HAFM appliance and the switch is down, the Hardware View displays the front and rear of the unit without FRUs. The switch **Status** table at the top of the Hardware View changes to display the status (No Link) and the associated reason with a yellow background. The name, description, and location fields are blank.

The Reason field on the switch **Status** table displays one of the following reasons when there are no links:

- **Never Connected**—A network connection was never established between the switch and the HAFM appliance or the CTP card has failed. Check the IP addresses, the Ethernet local area network (LAN) physical connection between the switch and HAFM appliance, and other network connection conditions.
- **Link Timeout**—The network connection that was established between the switch and HAFM appliance has been lost. Check the IP addresses, the Ethernet LAN physical connection between the switch and HAFM appliance, IP addresses, and other network components.
- **Protocol Mismatch**—The switch and the HAFM appliance are not at compatible software release levels. Update the HAFM software version or your product's firmware so that they are at compatible levels.
- **Duplicate Session**—A link has previously been established between the switch and another instance of the HAFM appliance. Connect to the previously established HAFM appliance from the HAFM login screen.
- **Unknown Network Address**—The address defined for the switch in HAFM could not be found in the domain name server (DNS). Either the name was mistyped when the switch was added to the application, or the name was not available from the DNS. Check the network IP address for the switch definition in HAFM by right-clicking the product icon and selecting **Properties**. The IP address displays in the **Network Address** field.
- **Incorrect Product Type**—The product at the configured network address is not a switch. Verify address, configuration, and product type.
- **Link Disabled**—The IP address of an open Element Manager was removed from the discover list.

### Status bar status indicator

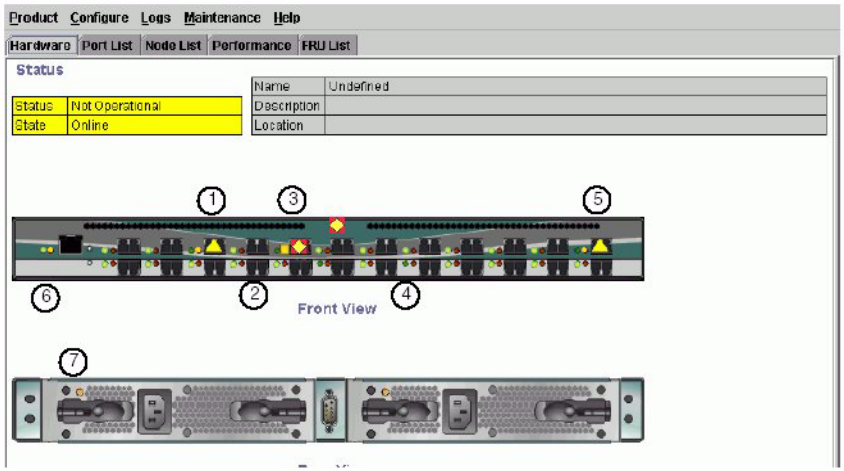
The status bar displays a colored status symbol that indicates the overall operating status of the switch unit. The operating status depends on hardware component failures, which are indicated by status symbols that display over component graphics in the **Hardware View**. See "Hardware View" on page 46 for the meanings of status symbols in the status bar.

The status bar indicates the switch operating status based on component failures. For example, a yellow triangle displays in the status bar to indicate a degraded switch. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a red and yellow diamond, indicating a failure that requires immediate attention.

## Monitoring hardware operation

You can determine hardware component operating status and states by viewing the simulated light emitting diode (LED) indicators and status symbols, such as flashing red and yellow diamonds and yellow triangles, that display on hardware components. These simulated LEDs and status symbols reflect the state of the actual hardware as changes occur. Corresponding or additional descriptions of hardware status and states also display when you double-click components to display Properties dialog boxes.

Figure 9 illustrates the Hardware View for the Edge Switch. The figure includes examples of symbols and LED indicators that display to help you monitor hardware operation. The numbers called out in Figure 9 are keyed to descriptions in the sections, "Front view" on page 48 and "Rear View" on page 49.




❶ Port Attention Indicator
❷ Port LED Indicator
❸ Port Failure Indicator
❹ Beaconing
❺ Not Installed
❻ Power, System Error, and Unit Beaconing Indicators
❼ Power Supply Status

**Figure 9** Hardware operation - Edge Switch Hardware View

## Front view

1. Port attention indicator

   The yellow triangle on the port connector graphic indicates that a link incident occurred or that the port is not operational, in nonstandard mode of operation, or has other status. You can determine the reason for a link incident by displaying the Port Properties dialog box for the port. For details on status symbols, see Table 4 on page 72. For information on link incidents, see "Link incident alerts" on page 75.

2. Port LED indicator

   The two round indicators (green or blue and amber) to the left of each port connector simulate LED operation on the actual switch port. A green LED indicates that the port is online with an operating speed of 1 gigabit per second (Gbps). A blue LED indicates that the port is online with an operating speed of 2 Gbps. When the amber indicator illuminates steadily, the port has failed and requires service. For details on port LED indicator operation, see Table 4 on page 72.

3. Port failure indicator

   A blinking red and yellow diamond over a port connector indicates that the port has failed. See Table 4 on page 72 for details on port operating states and the status symbol and indicator operation.

4. Beaconing

   When a blinking amber LED indicator displays by a port and a yellow triangle attention indicator displays over the port's connector, beaconing is enabled. See Table 4 on page 72 for details on port operating states and the status symbol and indicator operation.

5. Not Installed

   The port optics are not installed, or the feature that provides additional port function is not enabled.

6. Power, system error, and unit beaconing indicators

   The green or amber indicators on the far left of the front view simulate the power and system error LEDs on the actual switch.

   - Power indicator—The green indicator (**PWR**) simulates the power LED on the actual switch. When the indicator illuminates, the switch is connected to facility AC power and is operational. The indicator will be on if either power supply is operating.
   - System error indicator—The amber system error light indicator (**ERR**) simulates the system error light on the actual switch. When this indicator illuminates, an event has occurred requiring immediate attention, such as a system, power supply/fan, or port failure. View details of system errors by selecting **Logs > Event Log** on the Element Manager menu bar. The indicator in the Hardware View and the LED on the actual unit remains illuminated until you clear the event by right-clicking on the front view away from a hardware component and clicking **Clear System Error Light**.
   - Unit beaconing indicator— The amber system error indicator blinks if unit beaconing is enabled. Enable and disable unit beaconing by right-clicking on the front view away from a hardware component and clicking **Enable Unit Beaconing**. You can only enable beaconing if there are no system errors (the system error indicator is off).

## Rear View

7. Power Supply Status

   Each AC power connector indicates the location of an internal power supply. An amber, service-required LED indicator is located in the upper left corner of each AC power connector. The indicator illuminates if the power supply has failed and requires service. The indicator is off if the power supply is active.

   When a red and yellow diamond displays on a power connector, the internal power supply for that connector has failed. Note that the switch operates with one power supply failure; however, you should replace the power supply as soon as possible to retain redundancy.

# Obtaining hardware information

The Element Manager enables you to display FRU information, port properties, and switch properties using the various dialog boxes available on the **Hardware View**.

# Displaying FRU Information

Display the FRU Properties dialog box using one of the following methods:

- Double-click a FRU, such as a power supply module illustrated in the **Hardware View**.
- Click a FRU in the **Hardware View**, then select **Product > FRU > FRU Properties**.
- Double-click on a row in the **FRU List** view.

The FRU Properties dialog box displays the FRU name, slot position relative to identical FRUs installed in the chassis, active or failed state, part number, and serial number.

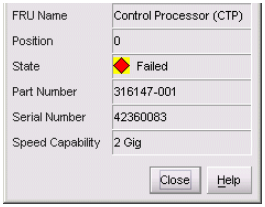



**Figure 10** FRU Properties dialog box

## Displaying port information

There are several ways to display the Port Properties dialog box:

- Double-click on a port connector in the Hardware View.
- Right-click on a port connector in the Hardware View and click **Port Properties** from the pop-up menu.
- Double-click on the port row in the Port List View table.
- Right-click on a port connector in the Performance View and click **Port Properties**.
- Right-click on a port's row in the Port List View and click **Port Properties**.
- Right-click on a port's row in the Node List View and click **Port Properties**.

- Click on a connector, port row, or bar graph in the preceding views or select **Product > Port > Port Properties**.

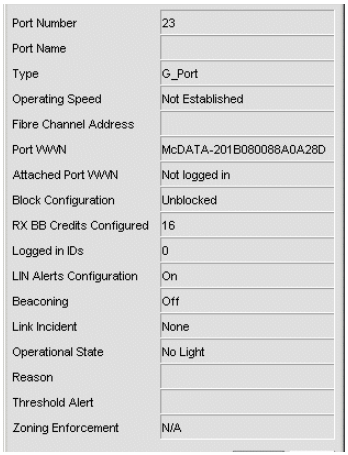



**Figure 11** Port Properties dialog box (Edge Switch 2/32)

## Port properties parameters

The Port Properties dialog box provides the following information in each of the listed fields:

- **Port Number**—The physical port number.
- **Port Name**—User-defined port name or description. See "Configuring ports" on page 84 for instructions.
- **Type**—Displays the port type, as follows:
  - G_port—Displays if nothing is logged into the port or the port is configured to be a G_Port.
  - F_Port—Displays if a device is logged into the port or the port is configured to be an F_Port.
  - E_Port—Displays if the port is connected to another switch's E_Port through an ISL or the port is configured to be an E_Port.
  - FL_Port—Displays if a loop device is logged into the port.
  - FX_Port—Displays if the port is configured to be an FX_Port.
  - GX_Port— Displays if the port is configured to be a GX_Port.
- **Operating speed**—Displays the current data speed for the port as **1 Gig**, **2 Gig**, or **Not Established**. **Not Established** displays if Negotiate was set for the port through the Configure Ports dialog box and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating.
- **Fibre Channel Address—**The switch's Fibre Channel address.
- **Port WWN**—The port's 16-digit World Wide Name (WWN).
- **Attached Port WWN**—The WWN of the node logged into the port.

- **Block configuration**—Blocked or unblocked. Operation can be blocked or unblocked using any of the following methods:
  - Through the Configure Ports dialog box. See "Configuring ports" on page 84 for instructions.
  - Right-click a port in the Hardware View, a port's row in the Port List View, or a port bar graph in the Performance View, and click **Block Port**.
  - Select **Product > Port > Block Port**. This option is available from the Hardware View, the Port List View, or the Performance View.
- **10-100 km configuration**—Extended distance buffering. This can be enabled or disabled for the port through the Configure Ports dialog box. See "Configuring ports" on page 84 for instructions.
- **RX BB Credits**—Indicates a switch that supports BB credit configuration.
- **LIN Alerts configuration**—Indicates whether LIN alerts are enabled or disabled. LIN alerts can be configured through the Configure Ports dialog box. The default is for the LIN alerts to be enabled.
- **FAN configuration**—Indicates whether Fabric Address Notification (FAN) is On or Off when the port is operating as an FL_Port.
- **Beaconing**—Indicates the beaconing status for the port. To enable or disable beaconing, right-click the port and click **Enable Beaconing**. (A port in a failed state cannot be set to beacon.)
- **Link incident**—Description of the last link incident that occurred on the port.
- **Operational state**—Beaconing, Inactive, Invalid Attachment, Link Incident, Link Reset, No Light, Not Operational, Online, Offline, Port Failure, Segmented E_port, Testing, Or Not Installed. See Table 4 on page 72 for definitions of operational states.
- **Reason**—When the port operating state is Segmented E_Port, Invalid Attachment, or Inactive, this field displays the reason for that state. When an E_Port is segmented, two fabrics are prevented from joining. This only occurs when the switch is connected to another switch.

  The following messages display in the **Reason** field of the Port Properties dialog box if an Invalid Attachment, Segmented E_Port, or Inactive state occurs for the port:

  Invalid attachment messages:

  - `01 Unknown`—The reason is not known.
  - `02 ISL connection not allowed on this port`—ISL is connected to a port configured as an F_Port.
  - `03 ELP rejected by the attached switch`—This switch transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL
  - `04 Incompatible switch other end of the ISL`—The switch is configured for Homogenous mode, and the switch at the other end of the ISL is an HP switch configured for Open Fabric 1.0 mode.
  - `05 External loopback adapter connected to the port`—A loopback plug is connected to the port, and no diagnostic test is running.
  - `06 N_Port connection not allowed on this port`—The port type configuration does not match the actual port use. (The port is configured as an E_Port, but attaches to a node device.)

- `07 Non-HP switch at other end of the ISL`—The cable is connected to a non-HP switch, and interop mode is set to Open Fabric 1.0 mode.
- `08 ISL connection not allowed on this port`—The port type configuration does not match the actual port use. (The port is configured as an F_Port, but attaches to a switch or director.)
- `10 Port binding violation - Unauthorized WWN`—The WWN entered to configure Port Binding for this port is not valid, or a nickname was used that is not configured for the attached device in the Element Manager.
- `11 Unresponsive node connected to port`—Possible causes are:
  - Hardware problem on switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login (FLOGI) cannot be received. There may be problems in the switch SBAR.
  - Faulty or dirty cable connection.
  - Faulty host bus adapters that do not send out FLOGI within a reasonable time frame.
- `0x0C ESA Security Mismatch`—Processing of Exchange Security Attribute Frame detected required security feature mismatch.
- `0x0D Fabric Binding Mismatch`—Fabric Binding is enabled and detected a switch connection with an incompatible fabric membership list. Could also be the result of problems delivering EFMD ILS.
- `0x0E Authorization Failure Reject`—The switch on the other side of the ISL detected a security violation. This switch receives notification via a generic reject reason code and sets its port to the invalid attachment state in sympathy.
- `0x0F Unauthorized Switch Binding WWN`—A Switch Binding error was detected on either an E_Port or F_Port.
- `0x10 Authentication Failure.` ISL Authentication Check (CHAP) failed—If you wish to allow the connection, update the authentication lists or disable authentication.
- `0x11 Fabric Mode Mismatch`—A connection was not allowed because:
  - An HP M-Series switch or director attempted to connect to an HP switch or director running in Open Fabric mode.
  - An HP M-Series switch or director running in Open Fabric mode attempted to connect to another vendor's switch or director with an incorrect ELP revision level.
- `0x12 CNT WAN Extension Mode Mismatch`—The ELP maximum frame sizes were incompatible because one product running in CNT WAN extension mode attempted to connect to another product running in a normal mode.

Segmented E_Port messages:

- `Incompatible operating parameters, such as resource allocation time-out values (R_A_TOV) or error-detect time-out values (E_D_TOV) are inconsistent`—See "Configuring operating parameters" on page 79 for more information.
- `Duplicate domain IDs`—See "Configuring operating parameters" on page 79 for more information.

- `Incompatible zoning configurations`—Refer to the *HP StorageWorks HA-Fabric SAN high availability planning guide* for information on joining zoned fabrics.
- `Build fabric protocol error.`
- `No principal switch (no switch in fabric is capable of being the principal switch).`
- `No response from an attached switch.`

- **Threshold alert**—If a threshold alert exists for the port, an alert indicator (yellow triangle) displays by the **Threshold Alert** field, and the configured name for the last alert received displays in the field.
- Zoning enforcement—For switches, this field displays **N/A**.

## Displaying switch information

Double-click the switch illustration (near to, but not on, a hardware component) to display the Switch Properties dialog box, as shown in Figure 12.

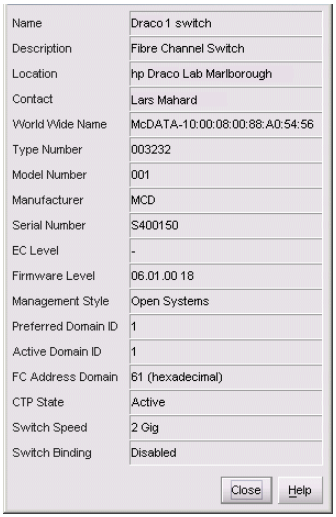



**Figure 12** Switch Properties dialog box (Edge Switch 2/32)

The following information displays in this dialog box:

- **Name**—Switch Name, description, location, and contact configured through the Configure Identification dialog box.
- **Type number**—Fibre Channel World Wide Name (WWN) identifier for the switch.
- **Type number**—Edge Switch type number.
- **Model number**—Product model number.
- **Manufacturer**—Product manufacturer.
- **Serial number**—Product serial number.
- **EC level**—Engineering change (EC) level.
- **Firmware level**—Firmware version number.

- **Management style**—Always set to the Open Systems management style.
- **Preferred domain ID**— As set through the Configure Switch Parameters dialog box.
- **Active domain ID**—The actual domain ID assigned to the switch.
- **FC address domain**—The switch's Fibre Channel address (hexadecimal).
- **CTP state**—Either Active or Failed.
- **Switch speed**—This is always set to `2 Gig`.
- **Switch binding**— Displays `Enabled` if the optional SANtegrity Binding features are installed and enabled. Otherwise, displays `Disabled`.

## Using menu options

Right-click on various parts of the Hardware View to display menu options for displaying status and information and for controlling the switch and various hardware components.Switch Menu

Right-click on any area of the switch illustration where a hardware component is not installed to display the following menu options:

- **Properties**—Displays the Switch Properties dialog box. This dialog box contains the switch name, description, location, and contact person configured through the Configure Identification dialog box. Also included is other product information, as detailed in "Displaying switch information" on page 54. You can also display this dialog box by double-clicking an area on the illustration (near to, but not on, a hardware component).
- **Enable unit beaconing**—Toggles unit beaconing on or off. When the check box has a check mark, unit beaconing is on, and the system error light (**ERR**) on the switch blinks to help users locate the unit managed by the Element Manager. The amber indicator on the Hardware View also blinks when beaconing is enabled. When you click the check box to remove the check mark, the unit beaconing is disabled.

**NOTE:** You can only enable beaconing if there are no system errors (the system error indicator is off).

- **Clear system error light**—Turns off the amber system error light (**ERR**), located below the green/blue power (**PWR**) LED on the switch. This also turns off the amber system error light indicator in the Hardware View (front view)
- **IPL**—Initiates an IPL on the switch. When the dialog box appears confirming the IPL, click **Yes**.

**NOTE:** An IPL is not intended for ordinary or casual use and should only be performed when directed by your support personnel.

See "Executing an IPL" on page 135 for detailed procedures.

- **Date/time**—To set the display and configure the date and time:

1. Click **Date/Time** to display the Configure Date and Time dialog box, as shown in Figure 13.

   The dialog box appears with a check mark (the default) in the **Periodic Date/Time Synchronization** check box. If this field is checked, the HAFM appliance periodically sets the switch time to automatically synchronize with the HAFM appliance time. Daylight savings time automatically updates on the switch when this option is used.

   The current date and time display in the **Date** and **Time** fields. If the **Periodic Date/Time Synchronization** field is checked, the **Date** and **Time** fields are disabled (grayed out).

   To enable and disable **Periodic Date/Time Synchronization**, click the check box and then click **Activate**.

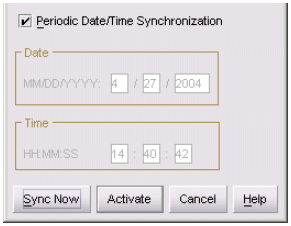



**Figure 13** Configure Date and Time dialog box

2. Perform one of the following steps:
   - To immediately synchronize the switch date and time with the HAFM appliance, make sure the **Periodic Date/Time Synchronization** option is enabled and then click **Sync Now**.

**NOTE:** If you enable the **Periodic Date/Time Synchronization** feature and click **Activate**, the time will synchronize at the next update period.

   - To set the switch with a specific date and time, make sure that the **Periodic Date/Time Synchronization** field is not selected, as shown in Figure 14. Enter the date and time, and then click **Activate**.

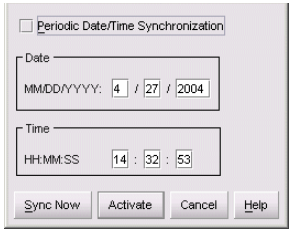



**Figure 14** Configure Date and Time (manually) dialog box

**NOTE:** Use the range of 0 to 23 for hours. Use the range of 0 to 59 for minutes and seconds.

- **Set Switch Online State**—Use the following procedure to set the online state of the switch.

△ **CAUTION:** Before setting the switch offline, warn administrators and users currently operating attached devices that the switch is going offline and that there will be a disruption of port operation. Also, request that the devices affected by an interruption of data flow be set offline.

1. Click to display the Set Online State dialog box. The dialog box displays the current state (offline or online) and provides a button for changing the state.
2. Click **Set Offline** or **Set Online** to toggle between the states.

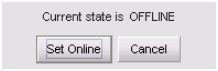



**Figure 15** Set Online State dialog box (switch is offline)

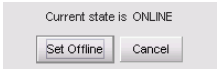



**Figure 16** Set Online State dialog box (switch is online)

3. When the **Set Online** or **Set Offline** warning dialog box appears, click **OK** to set the switch online or offline.

   As the switch goes offline, the word `OFFLINE` displays in the **State** field in the left corner of the **Hardware View**. As the switch goes online, the word, `ONLINE` displays in the **State** field in the left corner of the **Hardware View**. When going offline, LED indicators on all ports with attached devices stay green/blue, but the switch sends offline sequences (OLSs) to these devices.

## Port menu

While in the **Hardware View**, right-click on any port to display the following menu options.

**Port Properties**—Click this to display the Port Properties dialog box. This dialog box displays technical information about the port. See "Displaying port information" on page 50 for more information.

**Node Properties** (Edge Switch 2/32 only)—Click this option to display the Node Properties dialog box. See "Displaying node properties" on page 65 for details.

**Port Technology** —Click this to display the Port Technology dialog box. This dialog box displays the following information:

- **Port number**—The physical port number.
- **Connector type**—Always LC.
- **Transceiver type**—Longwave laser LC or shortwave laser LC.

- **Distance**—General distance range for port transmission. This can be either short to long distances for longwave laser LC transceivers or short distances for shortwave laser LC transceivers.
- **Media**—The Fibre Channel mode and optic size. For the longwave laser LC transceiver, this would be singlemode 9-micron. For the shortwave laser LC transceiver, this would be multimode 50-micron or 62.5-micron.
- **Speed**—This will be either 1Gbit per second or 1Gbit per second, 2 Gbit per second. Note that only 1 Gbit per second ports operate in the 1 Gbit switches.
- **Block port** —Click this option to display a check mark and block port transmission. If the port is blocked, a node attached to the port is prevented from logging into the switch or communicating with other devices attached to switch ports. A blocked port continuously transmits offline signals (OLSs). Click to remove the check mark and unblock the port. If the port is unblocked, a node attached to the port can communicate with the switch and can communicate with other nodes attached to the switch.
- **Enable beaconing**—Click this option to make the amber LED by the port blink on the actual switch and to make the amber indicator blink for the port in the Hardware View. This enables users to locate the unit where the port is located. When a blinking amber LED indicator displays by a port, an attention indicator displays below the port's connector in the Hardware View and on the port's row in the Port List View.
- **Channel Wrap (FICON management style only)**—Click this while in FICON management style to display a check mark and allow a channel wrap test to be initiated from an attached host or device. In this test, frames are sent to the switch port, then the switch echoes the frames back to the sending device to test the channel. The switch remains in channel wrap mode until the option is disabled. While in channel wrap mode, the port can only accept echo commands from the host and will appear to be blocked to all other communication. Click the check box to remove the check mark and disable channel wrap.
- **Port(s) Diagnostics**—Click this option to display the Port Diagnostics dialog box. Use this dialog box to run an internal loopback and external loopback test on the port. The **Port(s) Diagnostics** option enables you to run internal or external loopback tests on any port. To use this option, follow the detailed steps in the appropriate service manual for your Edge Switch.
- **Clear Link Incident Alert(s)**—Click this option to clear the attention indicator on the Hardware View, the Port List View, and the Performance View. In addition, the procedure clears the alert description in Port Properties dialog boxes. If there are no link incident alerts set for a port, no actions occur. Although you can manually clear link incidents, they may also be cleared by actions outside of the user interface, such as when the HAFM appliance is rebooted.
- Reset **Port**—Click this option to display a confirmation dialog box. Click **Yes** to reset the port. If a switch is attached to the port and is online, this operation sends a link reset to the attached switch; otherwise, this action disables port beaconing for the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state, clearing the service required (amber) LED. The reset does not affect other ports in the switch.

- **Port Binding**—Click this option to display the Port Binding dialog box (Figure 17). Use this dialog box to allow a device with a specific WWN or nickname to have exclusive connection to a port.

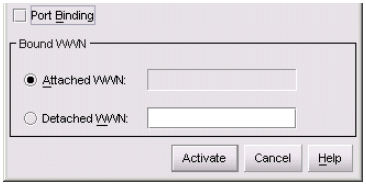



**Figure 17** Port Binding dialog box

Use the Port Binding dialog box to set the following options:

- **Port Binding**—Click this check box to place check mark in the box and enable Binding for the port. When Port Binding is enabled, only a specific device can communicate through the port. This device is specified by the WWN or nickname entered into the **Bound WWN** field (either the **Attached WWN** or **Detached WWN** options). With the check box cleared, any device can communicate through the port, even if a WWN or nickname is specified in the **Bound WWN** field.
- **Attached WWN**—When you click this button and, if a device is logged into the port, the device's WWN will display in the field. The device with this WWN or nickname will have exclusive communication privileges to the port if Port Binding is enabled.

---

**NOTE:** If you click this option button to bind the port to a logged-in device and there are no devices logged in, the port is essentially bound to a WWN of `0`. This prevents any device from logging in until this button is re-enabled to bind the WWN of a logged-in device or until you explicitly bind the WWN of a device by clicking the WWN option button and entering a WWN or nickname (see the following). Changes only take effect when you click the **Activate** button.

---

- **Detached WWN**—Click this option and enter a WWN in the proper format (`xx.xx.xx.xx.xx.xx.xx.xx`) or a nickname configured through the Product or HAFM. The device with this WWN or nickname will have exclusive communication privileges through the port if **Port Binding** is enabled.

  Note the following:

  - If you do not enter a valid WWN or nickname in this field, but the **Port Binding** check box is checked (enabled), then no devices can communicate over the port.
  - If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can communicate over the port.

- **Activate**—Click this button to activate settings in this dialog box.

  Warning and error messages display under the following circumstances:

  - If one or more of the nodes logged into a port does not match the WWN or nickname configured in the field by the **WWN** option button, a warning dialog box appears after you activate the configuration. This warning box displays a list of all nodes that will be logged off if you continue. If you click **Continue** on the warning box, these nodes will be logged off and the port will only attach to the device with the WWN or nickname configured in the **WWN** field.
  - An error message displays after you activate the configuration if the format for the WWN entered in the **WWN** field is not valid (not in `xx.xx.xx.xx.xx.xx.xx.xx` format) or if you have entered a nickname that was not configured through the Element Manager.

- **Clear Threshold Alert(s)**—Click this option to display the Clear Threshold Alert(s) dialog box. Click the appropriate option to clear alerts for the selected port only or for all ports on the switch. This clears all attention indicators that notify users of threshold alerts in dialog boxes and views. This action also restarts the notification interval and the cumulative minutes for utilization % interval.


Figure 18 Clear Threshold Alert(s) dialog box

# Port List View

Display the Port List View (Figure 19) in the View panel by clicking the **Port List View** tab on the Element Manager window.

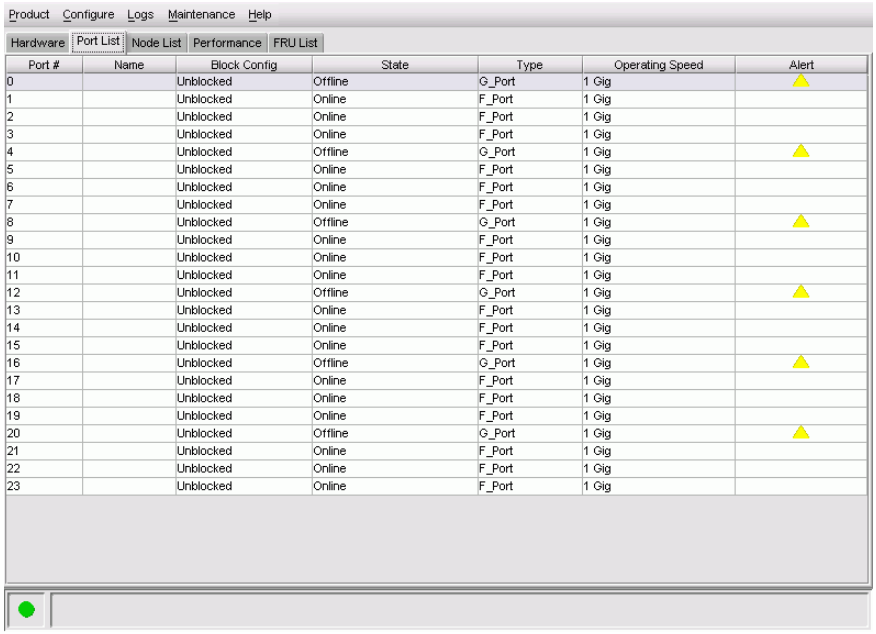



**Figure 19** Port List View

## Port List View parameters

The Port List View displays a table with columns. The columns display information on all ports that can be installed in the switch. This display is updated automatically. The following lists each column and explains the type of information it displays:

- **Port #—**Displays number of the port, from 0 through 23 for the Edge Switch 2/24 or 0 through 31 for the Edge Switch 2/32.
- **Name**—Displays the port name, as configured through the Configure Ports dialog box.
- **Block Config**—Indicates the blocked or unblocked configuration of the port, as set through the Configure Ports dialog box.

  The **Block Port** option is available by right-clicking the port in the **Hardware View**, the port row in the **Port List View**, or the port bar graph in the **Performance View**. Or, you can select **Product > Port**.

  Blocked states are:

  - **Blocked**—Devices communicating with the port are prevented from logging into the switch or communicating with other devices attached to switch ports. A blocked port continuously transmits an offline signal (OLS).
  - **Unblocked**—Devices communicating with the port can log in to the switch and communicate with devices attached to any other unblocked port in the same zone.

- **State**

  The following port operational states may display in this table. For more information on these states and corresponding status symbol and LED indicator operations in the **Hardware View**, see "Port operational states" on page 72.

  - No Light
  - Online
  - Offline
  - Beaconing
  - Link Reset
  - Not Operational
  - Not Installed
  - Invalid Attachment
  - Port Failure
  - Segmented E_Port
  - Link Incident
  - Testing
  - Inactive
- **Type**—The type of port:
  - If the **Port State** is online, the available port types are **F_Port**, **FL_Port**, and **E_Port**.
  - If the **Port State** is not online, the available port types are the configured types: **Gx_Port**, **G_Port**, **Fx_Port, F_Port,** and **E_Port**.
- **Operating Speed**—This column indicates the speed at which the port is operating. Possible values are 1 Gb/sec, 2 Gb/sec, and Not Established.
- **Alert**—This column displays a yellow triangle if a link incident or other alert occurs on the port or if the port's LED is beaconing. Blinking red and yellow diamonds display for port failures or for ports requiring service. Click the row to display the reason for the alert in the Port Properties dialog box.

Double-click a row to display the Port Properties dialog box. For an explanation of the fields on the Port Properties dialog box, see "Displaying port information" on page 50.

## Port List Menu options

Right-click a row to display a menu with port-related options. These are the same menu options that display when you right-click a port in the Hardware View and Performance View. You can also display this menu by clicking on a port, port row, or port graph in the preceding views and selecting **Product > Port**.

See "Port menu" on page 57 for an explanation of the menu options.

# Node List View

Display the Node List View by clicking the **Node List View** tab on the Element Manager window. This view displays, in table format, information about all node attachments to F_Ports and FL_Ports on the switch, sorted by port number. All data is dynamic and updates automatically as devices log in and log out.

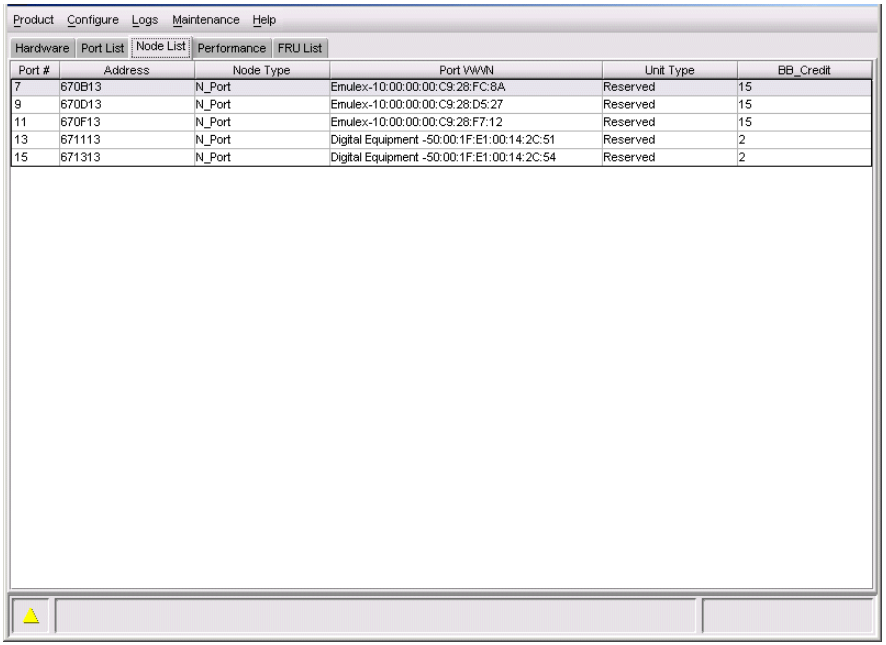



**Figure 20** Node List View (Edge Switch 2/24)

## Node List View parameters

The following lists the columns in the Node List View and the information that each displays for each node:

- **Port #**—Number of the port, from 0 through 23 in the Edge Switch 2/24 or 0-31 in the Edge Switch 2/32.
- **Address**—The 3-byte Fibre Channel address for the node or the arbitrated loop physical address (ALPA) for private loop devices.

- Node Type (Edge Switch 2/24 only)—The node type:
  - N_Port—The switch port is operating as an F_Port.
  - NL_Port—the switch port is operating as an FL_Port
- **Port WWN**—The port WWN of the attached node (N_Port). The 16-digit WWN is a set of unique numbers assigned to the device attached to the port. The WWN is prefixed by the manufacturer's name of the host bus adapter that attaches to the device. If there is a nickname assigned, the nickname displays instead of the WWN. For private loop devices, `Not Logged In` displays.
- **Unit Type**

  The following information, if supported, is supplied by the attached device:
  - Converter
  - Gateway
  - HBA
  - Module
  - Other
  - Proxy-agent
  - Storage device
  - Software driver
  - Storage subsystem
  - Switch
  - Unknown

**NOTE:** The Unit Type comes directly from the device's sense ID when the device attaches to the port during login. If the connection is lost to the device, the type will display as `Unspecified`, because the device is no longer logged into the port. When the device logs back in, the unit type updates.

- **BB_Credit**—The BB_Credit supported by the device. This field is left blank for all loop devices.

Double-click a row to display the Node Properties dialog box. For an explanation of the fields on the Node Properties dialog box, see "Displaying node properties" on page 65.

**NOTE:** Private loop devices do not log into the fabric and do not provide any additional information other than their Arbitrated Loop Physical Address (ALPA) for private loop devices. The Port WWN field displays `Not Logged In` and the Unit Type field is blank for all private loop devices.

## Node List View Menu options

In the Node List view, right-click a row to display a menu with the following port-related options:

- **Node Properties**—Click this option to display the Node Properties dialog box. See "Displaying node properties" on page 65 for details.
- **Port Properties**—Click this option to display the Port Properties dialog box (see Figure 11 on page 51).
- **Define Nickname**—Click this option to display the Define Nickname dialog box, where you can define a nickname to display for the attached device instead of the device's 8-byte WWN.

  The Define Nickname dialog box displays the WWN of the device attached to the port. To define a nickname, enter a name of up to 24 characters in the **Nickname** field and click **OK**. The nickname will display under the **Port WWN** column instead of the device's WWN. (You can configure a maximum of 2,048 nicknames.)
- **Display Options**—Click **Nickname** or **Worldwide Name** from the submenu. Clicking **Nickname** displays attached devices in the **Port WWN** column by the nickname configured through the **Define Nickname** menu option. Clicking **Worldwide Name** displays attached devices in the **Port WWN** column by the device's WWN.

  Note that you can also display these menu options by clicking a port row and then clicking the **Product > Port**.

## Displaying node properties

Open the Node Properties dialog box by double-clicking a row in the Node List View or right-clicking a row and clicking **Node Properties**.

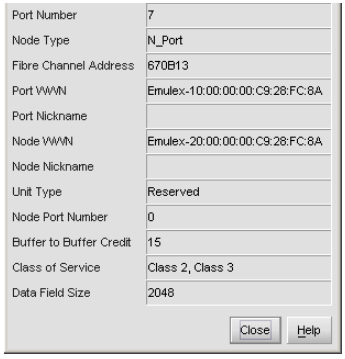



**Figure 21** Node Properties dialog box

The Node Properties dialog box contains the following options:

- **Port Number**—The physical port number on the switch to which the node is connected.
- **Node Type**—The type of port, as supplied by the attached port.
- **Fibre Channel Address**—The 3-byte address of the node or the ALPA for private loop devices.
- **Serial Number**—product serial number.
- **Port WWN**—Port WWN of the attached device.

- **Port Nickname**—Nickname for the port WWN. Must be configured to display.
- **Node WWN**—Node WWN of the attached device. Must be configured to display.
- **Node Nickname**—Nickname for the node WWN.
- **Unit Type**—Type of device. For a list of options, see "Unit Type" on page 64.
- **Node Port Number**—Physical port number on the attached node (if supplied by the device).
- **Buffer to Buffer Credit**—The buffer-to-buffer credits that the attached node has available. These credits determine the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device.
- **Class of Service**—This can be Class 2, Class 3, or both.
- **Data Field Size**—The largest size of Fibre Channel frame that the node will process. The size is negotiated with the attached device.

# Performance View

Display the Performance View by clicking the **Performance** view tab in the Element Manager window. This view displays a bar graph at the top of the view for each port. The lower portion of the view displays statistical values for the specific port's bar graph that you select.

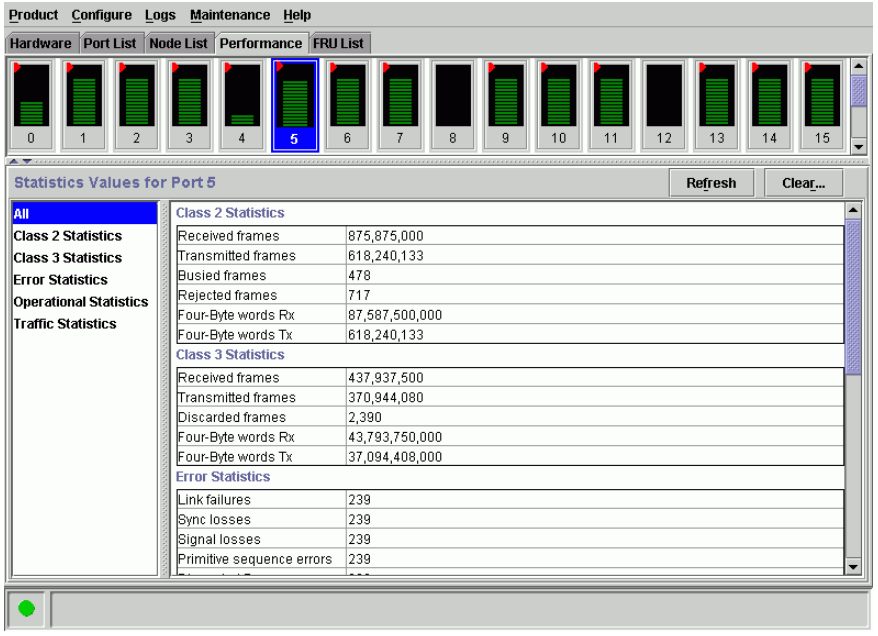



**Figure 22** Performance View

## Performance View Menu options

Right-click any of the port bar graphs to display a menu with the following port-related action options. These are the same menu options that display when you right-click a port in the Hardware View or on a row in the Port List View. You can also display these options by clicking a port, port row, or port bar graph in the Hardware View or Port List View and selecting **Product > Port**.

See "Port menu" on page 57 for an explanation of the menu options.

## Bar graph display

The Performance View provides a graphical display of performance for all ports. Each bar graph in the upper portion of the View panel displays the percentage of link utilization for the port. This information updates every five seconds. A red arrow marks the highest utilization since the opening of the Performance View. If the system detects activity on a port, it represents minimal activity with one bar.

When a port is operating as an F_Port and a device is logged on, moving the mouse pointer over the port's bar graph displays a message with the attached port's WWN. If the port is an E_Port, the message reads `E_Port`. If the port is an FL_Port, `FL_Port` displays. If the port is not logged in, the message displays the port's current operational state (see Table 4 on page 72).

Display the Performance View in the View panel by clicking the **Performance** view tab in the Element Manager window.

## Port statistics

To display more detailed performance information for a port, click the port's bar graph. The bar graph for that port highlights with a darker background, and the lower portion of the Performance View tab displays the statistics values for the port's number and the WWN decoding.

The **Statistics Values** tables contain a menu of specific statistics that can be displayed: **All**, **Class 2 Statistics**, **Class 3 Statistics**, **Error Statistics**, **Operational Statistics**, and **Traffic Statistics**.

Click a category in the left frame of the statistics area to display only statistics for that category, or click **All** to display values for all categories. For a description of the **Refresh** and **Clear** buttons, see "Button functions" on page 70.

### Statistics description

The **Statistics Values** tables contain statistics in the following groups. To refresh tables with the latest data, click the **Refresh** button on the upper right portion of the **Statistics Values** panel, or click the port's bar graph. Clear all counters for all users by clicking **Clear**.

#### Class 2 Statistics

The **Class 2 Statistics** table includes:

- **Received Frames**—The number of Class 2 frames received by this port from its attached port.
- **Transmitted Frames**—The number of Class 2 frames transmitted by this port to its attached port.

- **Busied Frames**—The number of F_BSY frames generated by this F_Port against Class 2 frames. This can occur if frames are received before the switch completes initialization or if the switch is servicing so many requests that it can not process a new request. The port generates frames if the switch is not ready to accept commands. This may indicate temporary congestion.
- **Rejected Frames**—The number of F_RJT frames generated by this F_Port against Class 2 frames.

  These frames usually occur because of attached device errors. The device is expected to correct the error based on the reject code, then retry its request. If the device is able to recover, there is no cause for concern. If not, further troubleshooting may be necessary. There are no thresholds for this value. Typically, this occurs because the destination is not available due to the device's action.
- **Four-Byte Words Rx**—The number of four-byte words received.
- **Four-Byte Words Tx**—The number of four-byte words transmitted.

### Class 3 Statistics

The **Class 3 Statistics** table includes:

- **Received Frames**—The number of Class 3 frames received by this port from its attached port.
- **Transmitted Frames**—The number of Class 3 frames transmitted by this port to its attached port.
- **Discarded Frames**—The number of Class 3 frames discarded, including multicast frames with bad destination identifiers (D_IDs).

  The switch increments this count when it discards a frame that cannot be routed. This occurs most frequently when a destination becomes unavailable without the source realizing that the destination is unavailable. There are no thresholds for this value. Typically, this occurs when the destination is not available due to the destination device's action.
- **Four Byte Words Rx**—The number of four-byte words received.
- **Four Byte Words Tx**—The number of four-byte words transmitted.

### Error statistics

Port errors indicate that a port is not operating correctly. Use this data to isolate problems with port and link operations. The statistics in this table include:

- **Link failures**—A link failure was recorded in response to a not operational sequence (NOS), protocol timeout, or port failure. At the Hardware View, a yellow triangle displays to indicate a link incident, or a blinking red and yellow diamond displays to indicate a port failure.
- **Sync losses**—A loss of synchronization was detected because the attached device was reset or disconnected from the port. At the Hardware View, a yellow triangle displays to indicate a link incident.
- **Signal losses**—A loss of signal was detected because the attached device was reset or disconnected from the port. At the Hardware View, a yellow triangle displays to indicate a link incident.

- **Primitive sequence errors**—An incorrect primitive sequence was received from the attached device, indicating a Fibre Channel link-level protocol violation. At the Hardware View, a yellow triangle displays to indicate a link incident.
- **Discarded frames**—A received frame could not be routed and was discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the switch.
- **Invalid transmission words**—The number of times that the switch detected invalid transmission words from the attached device. This indicates that a frame or primitive sequence arrived at the switch's port corrupted. This corruption can be due to the attached device performing a reset, plugging or unplugging the link, bad optics at either end of the cable, a bad cable, or a dirty or poor connection. Moving the connection around or replacing cables can isolate the problem.

  Some number of invalid transmission words are expected and acceptable. Invalid transmission words within a frame are used to produce the bit-error threshold link incident. If one or more invalid transmission words are detected in 12 separate 1.5-second samples within 5 minutes, a bit-error threshold link incident is generated.
- **CRC errors**—A received frame failed a cyclic redundancy check (CRC) validation, indicating that the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors**—The number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid Class of Service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, a bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors**—A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates that the destination device is unavailable.
- **Frames too short**—A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating that the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

### Operational statistics

The following describes the Operational Statistics that display for a selected port:

- **Offline sequences Rx**—The number of offline sequence that the port has received.
- **Offline sequences Tx**—The number of offline sequence that the port has transmitted.
- **Link resets Rx**—The number of link reset protocol frames received by this port from the attached device. The switch receives a link reset from an attached device if the device wishes to initiate the link reset or recover from a link timeout.
- **Link resets Tx**—The number of link reset protocol frames received/transmitted by this port from/to the attached device. The switch transmits a link reset to initiate the link reset protocol or

recover from a link timeout. This occurs normally to establish BB_Credit on any port in order to recover lost BB_Credit.

- **LIPS detected**—A loop initialization primitive was detected, which means the loop was completed.
- **LIPS generated**—A loop initialization primitive was created to initialize a loop.

### Traffic statistics

This section describes the types of statistics that display when you click a port's bar graph:

- **Link Utilization % Rx** and **Link Utilization %Tx**—There is a separate value for receive link utilization and transmit link utilization. The larger of these two values displays on the bar graph.

  The current link utilization for the port is expressed as a percentage. This statistic shows the percentage of the maximum link utilization currently being used. (If the port speed is 1 Gb/s, the quantity of the maximum link utilization is 100 MB. If the port speed is 2 Gb/s, the quantity of the maximum link utilization is 200 MB.) Link utilization is calculated over one-second intervals. The maximum link utilization is 100%.
- **Frames Rx**—The number of frames that the port has received.
- **Frames Tx**—The number of frames that the port has transmitted.
- **Four Byte Words Rx**—The number of words that the port has received.
- **Four Byte Words Tx**—The number of words that the port has transmitted.
- **Flows rerouted from ISL**—The number of Fibre Channel traffic flows that were rerouted from this ISL to another ISL due to congestion. This value increments only if the Open Trunking feature is installed. A value would display only if this port is connected to an ISL.
- **Flows rerouted to ISL**—The number of Fibre Channel traffic flows that were rerouted to this ISL from another ISL due to congestion. This value increments only if the Open Trunking feature is installed. A value would only display if this port is connected to an ISL.

## Troubleshooting tips

As a general rule, you should clear all counts after the system is stabilized. When looking at the Performance View, roughly keep track of the time interval when errors accumulate to judge the presence and severity of a problem. Also, recognize that there is a link recovery hierarchy implemented in Fibre Channel to handle some level of "expected anomalies." In general, only be concerned with error counts that increment very quickly.

## Button functions

The two buttons located at the right end of the title bar on the **Statistics Values** table are:

- **Refresh**—Updates the data in the statistics tables and enables you to compare values at any given time. Note that you can also refresh data by clicking the port's bar graph.
- **Clear**—Clears all counters to zero. Clicking this button displays a Clear Port Statistics dialog box. Click the appropriate option button and click **OK** to clear all counters to zero on the selected port only or all counters on all ports on the switch. Note that this also clears counters for other Element Manager users.

Click **Clear** to clear the statistics counters to zero. When the confirmation dialog box appears, click **This port only** or **All ports on product**, then click **OK** to clear the counters to 0.

An entry identifying when the statistics were cleared, and by whom, is saved in the Audit Log.

# FRU List View

Display the **FRU List** in the main panel by clicking the **FRU List** tab on the Element Manager window. This view displays information about all installed FRUs on the switch. All data is dynamic and updates automatically as the software detects changes.

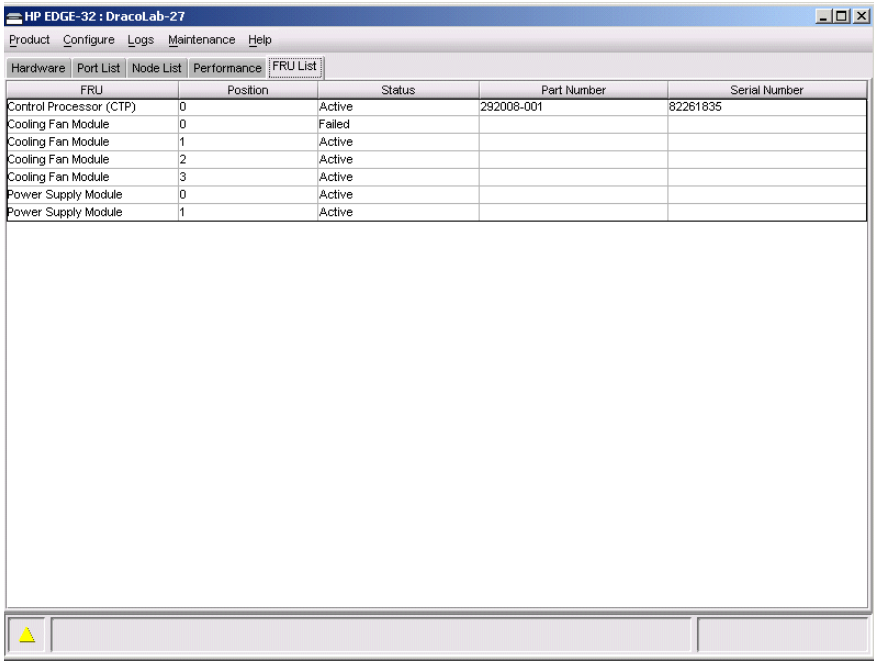



**Figure 23** FRU List View

Information on the FRU List View for each FRU includes:

- **FRU Name**—Control Processor (CTP), Cooling Fan, and Power Supply Module. Note that the CTP is an internal component, and if it fails completely the entire switch must be replaced. The meanings of FRU acronyms are:
  - **CTP**—CTP card
  - **FAN**—Fan module
  - **PWR**—Power supply
- **Position**—Slot position of FRU in the chassis relative to identical FRUs also installed in the chassis.
- **Status**—Active or failed. `Active` displays always unless the FRU fails. `Failed` displays if the FRU is not functional.
- **Part Number**—Part number of the FRU.

- **Serial Number**—Serial number of the FRU.

You can display the FRU Properties dialog box for a specific FRU by using one of the following methods:

- Double-click on the FRU row.
- Click a row in the FRU List View and then select **Product > FRU > Properties**.

## Port operational states

Table 4 describes the port operational states and the LED and attention indicators that display in the Hardware View and Port List View.

**Table 4** Port states and indicators

| Port state | Green/blue port indicator | Amber port indicator | Alert indicator* | Description |
|---|---|---|---|---|
| Beaconing | Off or On | Blinking | Yellow Triangle | The port is beaconing. The amber port LED blinks once every two seconds to enable users to find a specific port. Enable beaconing through the port's menu on the Hardware View, Port List View, or Performance View. |
| Inactive | Off | Off | Yellow Triangle | The switch port is in an inactive state. Reasons for this state display in the **Reason** field of the Port Properties dialog box.<br>Note that if port optics have also failed, the amber LED will be on. |
| Invalid Attachment | On | Off | Yellow Triangle | The switch port is in an invalid attachment state. Reasons for this state display in the **Reason** field of the Port Properties dialog box. |
| Link Incident | Off | Off | Yellow Triangle | A link incident occurred on one of the ports and displays in the Port List View, with a corresponding indicator displaying for the card in the Hardware View. |
| Link Reset | Off | Off | Yellow Triangle | The switch and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state that should not persist. |
| No Light | Off | Off | None | No signal (light) is being received on the switch port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off. |
| Not Operational | Off | Off | Yellow Triangle | The switch port is receiving the Fibre Channel not operational sequence (NOS) indicating that the attached device is not operational. |

**Table 4** Port states and indicators (continued)

| Port state | Green/blue port indicator | Amber port indicator | Alert indicator* | Description |
|---|---|---|---|---|
| Online | On | Off | None | The attached device has successfully connected to the switch and is ready to communicate or is in the process of communicating with other attached devices. As long as the port remains in the online state, the green/blue port LED remains illuminated. Note that on the actual port in the unit, the green/blue LED blinks when there is active Fibre Channel traffic through the port. |
| Offline | Off | Off | None | The switch port was configured as "blocked" and is transmitting the Fibre Channel OLS to the attached device. |
| | Off | Off | Yellow Triangle | The switch port was configured as "Unblocked" and is receiving the Fibre Channel OLS, indicating that the attached device is offline. |
| Port Failure | Off | On | Red and Yellow Blinking Diamond | The switch port has failed and requires service. The amber LED for the port remains illuminated. |
| Segmented E_Port | On | Off | Yellow Triangle | The E_Port is segmented preventing the two fabrics from joining (this only occurs when two switches are connected to each other). Display the Port Properties dialog box to view the segmentation reason. |
| Testing | Off | Blinking | Yellow Triangle | Port is executing an internal loopback test. |
| | On | Blinking | Yellow Triangle | Port is executing an external loopback test.<br>Note: For any loopback test, the amber LED blinks (beacons) to help users locate the port under test. |
| Not Installed | Off | Off | None | The port optics are not installed, or the feature that provides additional port function is not enabled. |

* The alert indicator displays on the port in the Hardware view. It indicates that a corrective action is required to return the port to a normal operating state.

**NOTE:** The status indicator displays on the port in the Hardware View. It indicates that a corrective action is required to return the port to a normal operating state.

## Link incident alerts

A link incident is a problem detected on a fiber optic link, like the loss of light, invalid sequences, and other problems. When a problem occurs, a LIN alert is sent to the Link Incident Log in the switch Element Manager. LIN alerts warn you that there is a link incident being detected through a port connection that may require operator intervention to correct.

If LIN alerts are enabled for a port in the Configure Ports dialog box, a yellow triangle (attention indicator) displays by the port connector in the Hardware View or in the **Alert** column in the Port List View. Double-clicking the port with the yellow triangle displays the Port Properties dialog box.

If LIN alerts have been enabled for a port in the Configure Ports dialog box, the Port Properties dialog box contains a short description of the latest incident in the **Link Incident** field. Or, if there are no active incidents, `None` displays. The system writes all link incidents to the Link Incident Log.

If you enable LIN alerts for a port in the Configure Ports dialog box, configure e-mail notification through HAFM, and enable **E-Mail Notification** through the **Maintenance** menu, you will receive e-mail notification of LIN alerts.

**NOTE:** The e-mail notification of LIN alerts is available to all users; no user permission levels are imposed.

Although you can manually clear the attention indicator in the Hardware View and the alert description in the Port Properties dialog box, they may also be cleared by actions outside of your control, such as on HAFM appliance reboot.

You can manually clear the link incident indicator in the Hardware View and the description in the **Link Incident** field. To manually clear the attention indicator (yellow triangle), right-click the port with the yellow triangle and click **Clear Link Incident Alert(s)**. In the Clear Link Incident Alert(s) dialog box, choose the appropriate option and click **OK**.

Be aware that clearing the incident indicator clears it for everyone using the system. If there are no link incident alerts enabled for a port, no actions occur.

# Threshold alerts

A threshold alert notifies Element Manager users when the transmit (Tx) or receive (Rx) throughput reaches specific values for switch ports or port types [E_Ports, F_Ports, or FL_Ports (Edge Switch 2/24 only)].

Select **Configure > Threshold Alerts** to display the Configure Threshold Alerts dialog box. Use this dialog box to configure criteria for generating a threshold alert. One criteria that you must configure is a throughput value that equals a specific percentage of the port's total throughput capacity. You also provide a time interval during which throughput is measured and a time interval during which that throughput value must remain constant. When throughput reaches the threshold value and remains constant for the specified time, an alert is generated.

Threshold alerts occur as the following in the Element Manager:

- An attention indicator (yellow triangle) that displays on the port in the Hardware View.
- An attention indicator (yellow triangle) that displays in the **Alert** column of the Port List View.
- An attention indicator (yellow triangle) that displays by the **Threshold Alerts** field in the Port Properties dialog box.
- Detailed threshold alert data recorded in the Threshold Alert Log.

For detailed procedures to configure threshold alerts, see "Configuring threshold alerts" on page 109.

# 3 Configuring the switch

This chapter describes how to configure the Edge Switch 2/24 or Edge Switch 2/32. It also includes information about backing up and restoring configuration data.

# Configuring identification

Use the procedure in this section to identify the switch by its name, description, location, and contact person. This information displays in the following Element Manager locations:

- Element Manager window title panel (name).
- The Switch Properties dialog box (name, location, contact, description).
- Identification table at the top of the Hardware View (name, location, description).

The name also displays in the switch icon label in the HAFM Physical/Topology Map, if the product name is enabled through the drop-down display list on the tool bar.

**NOTE:** Data entered through the following procedure is saved in nonvolatile random access memory (NV-RAM) on the switch.

To configure identification for the switch, use the following steps:

1. Select **Configure > Identification**. The Configure Identification dialog box appears.

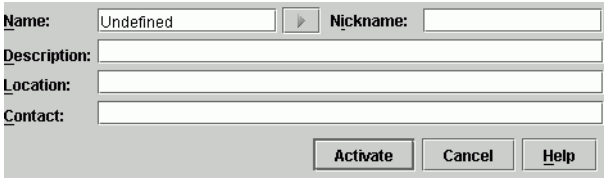



**Figure 24** Configure Identification dialog box

2. Click in the **Name** box and enter a name for the switch of up to 24 alphanumeric characters. The name could reflect the switch's Ethernet network domain name service (DNS) host name, if assigned.
3. Click in the **Nickname** box and enter a nickname for the switch of up to24 alphanumeric characters. The nickname will display instead of the WWN in Element Manager views. (You can configure a maximum of 2,048 nicknames.)
4. Click in the **Description** box and enter a description of the switch of up to 255 characters.
5. Click in the **Location** box and enter the location of the switch of up to 255 characters.
6. Click in the **Contact** box and enter up to 255 characters of appropriate information about a contact person, such as a phone number, title, or e-mail address.
7. Click **Activate** to save the data and close the dialog box.
8. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

# Configuring operating parameters

Use the procedures in this section to set parameters on the switch for switch and fabric operation. These operating parameters are stored in NV-RAM on the switch.Configuring Switch Parameters

Use procedures in this section to set parameters on the switch for switch operation through the Configure Switch Parameters dialog box.

To set switch parameters:

**NOTE:** The switch must be offline to change Preferred Domain ID. If it is not and you activate values in this dialog box, a dialog box appears, prompting you to set the unit offline.

**CAUTION:** Setting the switch offline terminates all Fibre Channel connections.

1. Set the unit offline:
   a. Select **Maintenance > Set Online State**.
   b. When the Set Online State dialog box appears, click **Set Offline**.
   c. When the warning box appears asking you to confirm the offline state, click **OK**.
2. Select **Configure > Operating Parameters > Switch Parameters**. The Configure Switch Parameters dialog box appears.

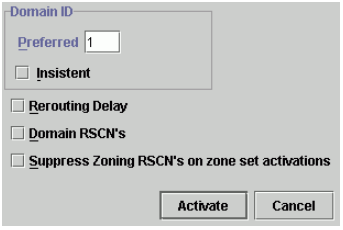



**Figure 25** Configure Switch Parameters dialog box

**NOTE:** You do not need to change values in this dialog box from their defaults. The only exception is the **Preferred Domain ID**. Change this value if the switch will participate in a multiswitch fabric.

3. Use information under "Switch parameters" on page 80 to change settings as required for parameters in this dialog box.
4. After you change settings, click **Activate**.

## Switch parameters

Configure the following parameters, as required by your fabric.

### Domain ID

The domain identification is a value (1 though 31) that provides a unique identification for the switch in a fabric. A fabric switch cannot contain the same domain ID as another switch or their E_Ports will segment when they try to join.

In the Configure Switch Parameters dialog box, a box is provided to enter a preferred domain ID and a check box is provided to enable this ID as an insistent domain ID.

### Preferred

Use this box to set each switch in the fabric to a unique preferred domain ID. Fibre Channel addresses in the switch include this preferred domain ID, which creates a unique identification for the switch in the fabric. The default value is 1. Set a preferred value of 1 through 31.

The preferred domain ID must be unique for each switch in a fabric. If two switches have the same preferred domain ID, the E_Ports segment, causing the fabric to segment.

### Insistent

Click the **Insistent** check box to remove or add a check mark. The default state is disabled (no check mark). When a check mark displays, the domain ID configured in the **Preferred Domain ID** box becomes the active domain identification when the fabric initializes.

**NOTE:** This option is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled. See "Configuring a Preferred Path" on page 144 for details.

**NOTE:** If you enable Insistent Domain while the switch or director is online, the Preferred Domain ID will change to the current active domain ID if the IDs are different.

**CAUTION:** If a switch with a duplicate domain ID exists in the fabric, both switches' E_Ports will segment when they try to join.

### Rerouting delay

To enable rerouting delay, place a check mark in **Rerouting Delay** check box. This option is only applicable if the configured switch is in a multiswitch fabric. The default state is disabled.

Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a

destination out of order because frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** box of the dialog box. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path.

### Domain RSCNs

Use this check box to enable domain register for state change notifications (domain RSCNs). Domain RSCNs are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBAs) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. For example, some HBAs may log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.

---

**NOTE:** This option is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

---

### Suppress zoning RSCNs on zone set activations

Fabric format domain register for state change notifications (RSCNs) are sent to ports on the switch following any change to the fabric's active zone set. These changes include activating and deactivating the zone set, or enabling and disabling the default zone. When the Suppress RSCNs on Zone Set Activations check box contains a check, fabric format RSCNs are not sent for zone changes to the attached devices on the switch. Click the check box to remove or add a check.

In general, RSCNs should not be suppressed, so that attached devices can receive notification of zoning changes in the fabric. However, some HBAs may log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic. Consult with your HBA and storage device vendor to determine if zone set change RSCNs will cause problems with your HBA or storage products.

## Configuring fabric parameters

The Configure Fabric Parameters dialog box enables you to configure the Fibre Channel operating parameters.

To set fabric parameters:

**NOTE:** The switch must be offline to change parameters in this dialog box. If it is not and you activate values in this dialog box, a dialog box appears, prompting you to set the unit offline.

**CAUTION:** Setting the switch offline terminates all Fibre Channel connections.

1. Set the unit offline:
   a. Select **Maintenance > Set Online State**. The Set Online State dialog box appears.
   b. Click **Set Offline**. A warning box appears asking you to confirm the offline state.
   c. Click **OK**.
2. Select **Configure > Operating Parameters > Fabric Parameters**. The Configure Fabric Parameters dialog box appears.

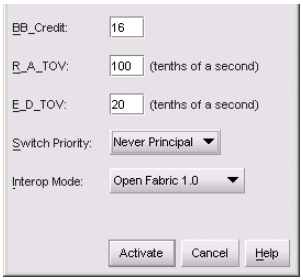



**Figure 26** Configure Fabric Parameters dialog box (Edge Switch 2/32)

**NOTE:** Ordinarily, you do not need to change values in this dialog box from their defaults. Change the values if the switch will participate in a multiswitch fabric.

3. Use information under "Fabric Parameters" on page 83 to change settings as required for parameters in this dialog box.
4. After you change settings, click the **Activate** button.

## Fabric Parameters

Configure the following parameters as required by your fabric.

### BB_Credit

(Edge Switch 2/32 only.) Buffer-to-buffer credit. This variable is used to set the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. Values range from 1 through 60. This value is used for all ports, except those configured for extended distance buffering (10-100 km). The default value is 16. For a description of buffer-to-buffer credit, refer to the industry specification, *Fibre Channel Physical and Signaling Interface*.

### R_A_TOV

Resource allocation time-out value. This variable is used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. Adjust the value for R_A_TOV in tenths of a second (100 ms) increments over a range of 10 tenths (1 second) to 1200 tenths (120 seconds). The default value is 100 tenths (10 seconds).

**NOTE:** Set the same value for R_A_TOV on all switches on a multiswitch fabric. If the value is not the same on all units, the fabric segments. Also, the value for R_A_TOV must be greater than the value configured for E_D_TOV.

### E_D_TOV

Error-detect time-out value. This defines the time that the switch waits for an expected response before declaring an error condition. Configure this value in tenths of a second (100 ms) increments in a range of 2 tenths of a second to 600 tenths (60 seconds). The default value is 20 tenths (2 seconds).

**NOTE:** Set the same value for E_D_TOV on all switches on a multiswitch fabric. If the value is not the same, the fabric segments.

### Switch Priority

Setting this value determines the principal switch for the multiswitch fabric. Click either **Principal** (highest priority), **Default**, or **Never Principal** (lowest priority) from the **Switch Priority** drop-down list.

If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest WWN becomes the principal switch.

Following are some examples of principal switch selections when switches have these settings:

- If you have three switches and set all to **Default**, the switch with the lowest WWN becomes the principal switch.
- If you have three switches and set two to **Principal** and one to **Default**, the switch with the **Principal** setting that has the lowest WWN becomes the principal switch.
- If you have three switches and set two to **Default** and one to **Never Principal**, the switch with the **Default** setting and the lowest WWN becomes the principal switch.

Note that at least one switch in a multiswitch fabric needs to be set as **Principal** or **Default**. If all of the switches are set to **Never Principal**, all of the interswitch links (ISLs) will segment. If all but one switch is set to **Never Principal** and the switch that was **Principal** goes offline, then all of the other ISLs will segment.

**NOTE:** HP recommends configuring switch priority as **Default**. If you are considering changing this value to something other than the default, refer to sections on principal switch selection for multiswitch fabrics in the *HP StorageWorks SAN high availability planning guide* for details.

In the audit log you may notice that the **Principal** setting maps to a number code of 1, **Default** maps to a number code of 254, and **Never Principal** maps to a number code of 255. The number codes 2-253 are no longer in use.

### Interop Mode

Choose one of the following modes:

- **Homogeneous Fabric**—Choose this mode if the fabric contains only HP directors and switches that are operating in Homogeneous Fabric mode.
- **Open Fabric 1.0**—Default. Choose this mode if the fabric contains HP directors and switches, as well as other open-fabric compliant switches. Choose this mode for managing heterogeneous fabrics.

## Configuring switch binding

For complete procedures on configuring this optional feature, see "SANtegrity features" on page 151.

## Configuring ports

The Configure Ports dialog box enables you to configure ports. Port configuration data is stored in NV-RAM on the switch.

The following sections describe the use of the Configure Ports dialog box:

- "Configuring ports parameters" on page 85
- "Configuring ports procedure" on page 88

## Configuring ports parameters

Configure data in the following columns of the Configure Ports dialog box:

- **Port #**—You cannot change this box. This column identifies the port number. The port numbers range from 0 through 23 for the Edge Switch 2/24 and 0 through 31 for the Edge Switch 2/32.
- **Name**—Enter a name of up to 8 characters for the port. The port names display in the Port Properties dialog box, and elsewhere in the Element Manager, to identify the port.

**NOTE:** To identify port numbers for which you want to provide names, place the mouse pointer over the ports in the Hardware View. As you move over a port, a label displays that identifies the slot number where the port is installed.

- **10-100Km**—This column is for extended distance buffering. You can enable extended distance for a port even if it is not an extended distance port. However, enabling extended distance buffering on a port disables the ability for the port to send broadcast traffic. When you select this option, the port can support up to 60 buffer-to-buffer credits (BB_Credits) to handle link distances up to 100 km. If this option is not enabled, the port uses the BB_Credit (1–60) configured through the Configure Fabric Parameters dialog box.

  If a device is connected and logged in to the fabric when extended distance is enabled or disabled on the corresponding port, the switch will send OLS for 5 ms to force the device to log in again and obtain the new BB_Credit value set for the port.

  Click **Activate** to display the 10-100Km confirmation dialog box.

**NOTE:** If a switch supports BB credits by port, an RX BB Credits column replaces the 10-100Km column.

- **RX BB Credit—** Minimum and maximum allowable port BB credit values vary by switch. If an invalid value is entered, an Invalid RX BB Credit error message displays. The BB credit value cannot be changed unless the port is offline. The BB Credit value is validated as entered. Click **Activate** to display the RX-BB Credit Confirmation box.

  In addition to the maximum BB credit limit per port, the total BB credits allocated to all ports cannot exceed the buffer pool size.

**NOTE:** Only 24-Port switches have a switch-wide buffer pool. The Configure Ports dialog box displays the total and available buffers at the bottom of the dialog box. When information is changed in the RX BB Credit column, this information also updates. If information is entered that exceeds the buffer pool and **Activate** is clicked, an error message displays. Also, ports for the 24-Port switches can be individually configured between 2-12, with a total number of port credits of 150.

Right-clicking in the RX-BB Credit column displays a RX BB Credits dialog box. For switches without buffer pools, this dialog box allows you to **Set all**. Set all sets all ports to a single value or **Set all to maximum** which set all ports to a maximum BB credit value. For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or to **Distribute** which evenly distributes the pool buffers among all ports. Clicking **OK** changes the values in the Configure Port dialog box. Clicking **Activate** changes the values on the Switch.

Clicking **Set all** displays the Set All RX BB Credits dialog box. Entering a value for RX BB Credit and clicking OK propagates the value to all ports on the Configure Ports dialog box. If an invalid value is entered, a message dialog box displays.

- **Blocked**—Placing a check mark in the check boxes in this column blocks the operation of the port.
- **LIN Alerts**—A link incident (LIN) is a problem detected on a fiber optic link, such as the loss of light or invalid sequences. When a problem occurs, a LIN alert is sent to the Link Incident Log in the switch Element Manager. LIN alerts warn you that there is a link incident being detected through a port connection.

  Place or remove check marks in the check boxes in this column to enable or disable link incident alerts. The factory default is to enable LIN alerts.

  A link incident causes a yellow attention indicator (triangle) to display for the port in the Hardware View and in the alert column of the Port List View. Once a LIN occurs, you can acknowledge it by clicking the **Clear Link Incident Alert** option from the right-click menu for the port (Hardware View). A description of the alert displays in the **Link Incident** box of the Port Properties dialog box (see Figure 11 on page 51).

  If the check boxes in this column are not selected, no link incident indicators display in the Hardware View. Also, the **Link Incident** box of the Port Properties dialog box is blank and a link incident is recorded in the Link Incident Log. LINs are always logged in the Link Incident Log, regardless of the configuration.

  If LIN Alerts are enabled, you can receive e-mail notification when a LIN occurs. In order to receive e-mail notification, you must configure and enable this feature in HAFM (**Monitor** menu) and enable e-mail notification through the **Enable E-Mail Notification** option on the Element Manager's **Maintenance** menu.

  For additional information about LIN alerts, see "Link incident alerts" on page 75.
- **FAN**—(Edge Switch 2/24 only.)Click to display a check mark in the check box and enable Fabric Address Notification for loop devices attached to the port. Right-click in this column to either clear all FANs for all ports or to set all FANs for all ports.
- **Type**—Click each port's type (G_Port, E_Port, F_Port, Fx_Port, or Gx_Port) in this column from the drop-down list. Right-click in this column to set all ports to either E_Ports, F_Ports, Fx_Ports, G_Ports, or Gx_Ports.

**NOTE:** If a switch's firmware level is below 6.0 and FICON management style is enabled, you cannot change port types unless the optional SANtegrity Binding feature is installed. If ports are configured as E_Ports in Open Systems management style, and you install SANtegrity Binding before changing to FICON management style, the ports will remain as E_Ports when you change to FICON management style. If SANtegrity Binding is not installed, setting a director to FICON management style will change all E_ports to G_Ports.

- **Speed**—Click the **Speed** column for a specific port, and choose **2 Gb/sec**, **1 Gb/sec**, or **Negotiate**. This sets the data rate for the port. Choosing **Negotiate** allows the port to negotiate the data speed with an attached device. Only set the speed to 2 Gb/sec on ports that support this speed. If the port optics do not support 2 Gb/sec, a warning displays stating that the optical transceiver in the port does not support the data rate.

  When you change a port's speed and click **Activate** on the dialog box, a confirmation message appears stating that this setting will temporarily disrupt port data transfers.
- **Port Binding** —Click this check box to display a check mark and enable Port Binding for the port. This allows only a specific device to attach to the port. This device is specified by the WWN or nickname entered into the **Bound WWN** column. With the check box cleared, any device can attach to the port, even if a WWN or nickname is specified in the **Bound WWN** column. Port Binding is allowed only for a port that is either a G_Port, E_Port, F_Port, or FL_Port.
- **Bound WWN**—Enter a World Wide Name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through HAFM. The device with this WWN or nickname will have exclusive attachment to the port if **Port Binding** is enabled. If a valid WWN or nickname is not entered in this box, but the **Port Binding** check box is checked (enabled), no devices can connect to the port. If you enter a WWN or nickname in this box and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can connect to the port.

# Configuring ports procedure

To configure ports, use the following steps:

1. Select **Configure > Ports**. The Configure Ports dialog box appears.

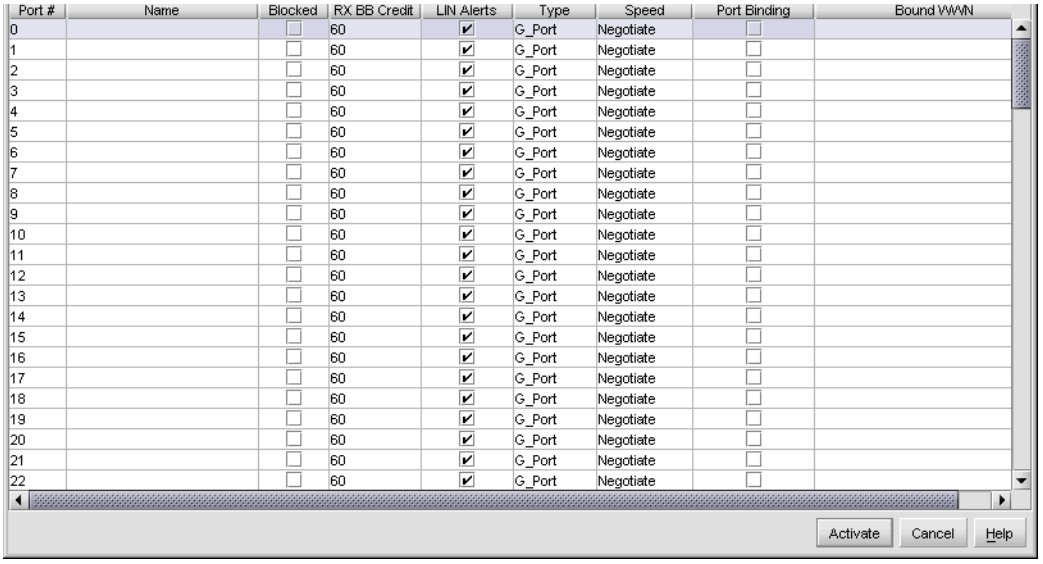



**Figure 27** Configure Ports dialog box (Edge Switch 2/32)

Ports are numbered from 0 through 24 for the Edge Switch 2/24 and 0 through 31 for the Edge Switch 2/32.

2. Click a **Name** box and type a name that reflects the end device connected through the port. For example, use `XYZ Server`, where XYZ is the brand name of the server.
3. Block or unblock operation for a port by clicking the check box in the **Blocked** column. When a check mark displays, the port is blocked.
4. (Edge Switch 2/32 only.) Enable or disable extended distance buffering for the port by clicking a check box in the **10-100 km** column. When a check mark displays, extended distance buffering is enabled.
5. If a switch supports BB Credit, the **RX BB Credit** column replaces the **10-100km** column. Use this to set minimum and maximum allowable port BB credit values as follows:

a. Right-click in the RX-BB Credit column to display the RX BB Credits dialog box as shown in Figure 28:

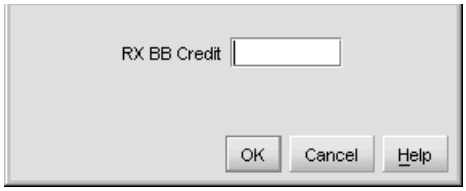



**Figure 28** RX BB Credit dialog box

Set the values as follows:

- For switches without buffer pools, use **Set all...** to set all ports to a single value or **Set all to maximum** which set all ports to a maximum BB credit value.
- For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or select **Distribute**, which evenly distributes the pool buffers among all ports.

b. Confirm your changes:

- Clicking **OK** changes the values in the Configure Port dialog box.

6. Clicking **Activate** changes the values on the switch.
7. Enable or disable LIN alerts for the port by clicking the check box in the **LIN Alerts** column. When a check mark displays, LIN alerts are enabled.

**NOTE:** The factory default for LIN alerts is enabled.

8. (Edge Switch 2/24 only.) Click a check box in the **FAN** column to enable Fabric Address Notification for loop devices.
9. Choose a port type by clicking in the **Type** box and selecting from the list.
10. To bind a device with a specific WWN or nickname to the port, click the **Port Binding** check box to display a check mark. Then enter the WWN or configured nickname for the device into the **Bound WWN** column. The device that you bind to the port will have exclusive connection to that port.

**NOTE:** If you have configured Port Binding and click **Activate**, a warning dialog box appears if one or more of the nodes attached to a port does not match the WWN or nickname configured in the **Bound WWN** column. This warning box displays a list of all attached nodes that will be logged off if you continue. If you click **Continue**, these nodes will log off and the port will only attach to the device with the WWN or nickname configured in the **Bound WWN** column.

If you have configured Port Binding and click **Activate**, an error message may display if the format for the WWN entered in the **Bound WWN** column is not valid (not in xx:xx:xx:xx:xx:xx:xx:xx format) or if you enter a nickname that has not been configured through the Element Manager.

11. To set the data speed for the port, click the **Speed** column for a specific port, and click **2 Gb/sec**, **1 Gb/sec**, or **Negotiate** (2 Gb/sec switch) or **1 Gb/sec only** (1 Gb/sec switch). Choosing **Negotiate** allows the port and attached device to negotiate the data rate.
12. Use the scroll bar on the right side of the Configure Ports dialog box table to display additional ports that you want to configure.
13. Activate changes and close the dialog box by clicking **Activate**.
14. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

# Configure Ports Procedure (Open Systems Management Style)

**NOTE:** This procedure applies only to the Edge Switch 2/32. Open Systems Management Style (OSMS) is not available on the Edge Switch 2/24.

To configure Edge Switch 2/32 ports in Open Systems management style, use the following steps:

1. Select **Configure > Ports**. The Configure Ports dialog box appears.

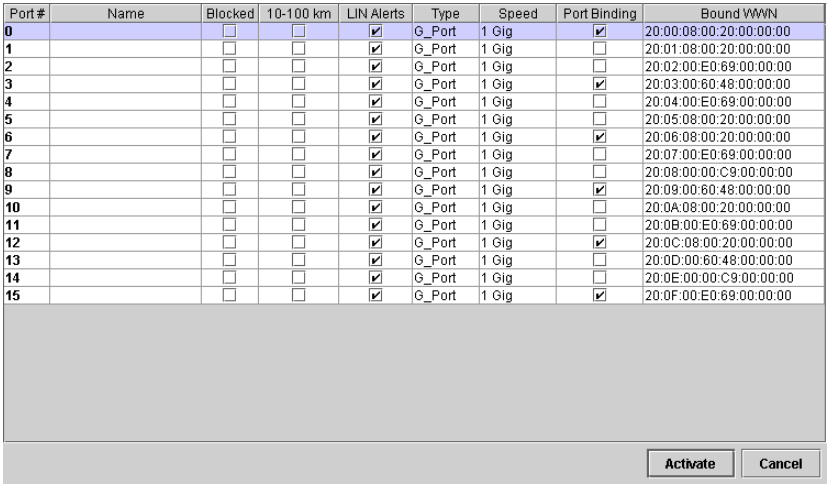



**Figure 29** Configure Ports dialog box (Open Systems Management Style)

Ports are numbered from 0 through 31.

2. Click a **Name** box and type a name that reflects the end device connected through the port. For example, use `XYZ` server. The `XYZ` is the brand name of the server.
3. Block or unblock operation for a port by clicking the check box in the **Blocked** column. When a check mark displays, the port is blocked.
4. Enable or disable extended distance buffering for the port by clicking the check box in the **10-100 km** column. When a check mark displays, extended distance buffering is enabled.

5. If a switch supports BB Credit, the **RX BB Credit** column replaces the **10-100km** column. Use this to set minimum and maximum allowable port BB credit values:
   a. Right-click in the RX-BB Credit column to display the RX BB Credits dialog box as shown in Figure 30:

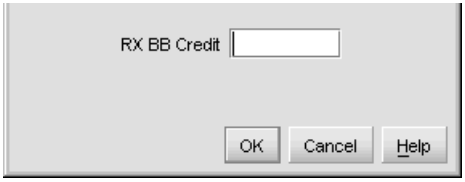



**Figure 30** RX BB Credit dialog box

   Set the values as follows:
   - For switches without buffer pools, use **Set all...** to set all ports to a single value or **Set all to maximum** which set all ports to a maximum BB credit value.
   - For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or select **Distribute**, which evenly distributes the pool buffers among all ports.

   b. Confirm your changes:
   - Clicking **OK** changes the values in the Configure Port dialog box.
   - Clicking **Activate** changes the values on the switch.

6. Enable or disable LIN alerts for the port by clicking the check box in the **LIN Alerts** column. When a check mark displays, LIN alerts are enabled.

**NOTE:** The factory default for LIN alerts is enabled.

7. Select a port type by clicking in the **Type** box and selecting from the list.
8. To bind a device with a specific WWN or nickname to the port, click the **Port Binding** check box to display a check mark. Then enter the WWN or configured nickname for the device into the **Bound WWN** column. The device that you bind to the port will have exclusive connection to that port.

**NOTE:** If you have configured Port Binding and click **Activate**, a warning dialog box appears if one or more of the nodes attached to a port does not match the WWN or nickname configured in the **Bound WWN** column. This warning box displays a list of all attached nodes that will be logged off if you continue. If you click **Continue**, these nodes will log off and the port will only attach to the device with the WWN or nickname configured in the **Bound WWN** column.

If you have configured Port Binding and click **Activate**, an error message may display if the format for the WWN entered in the **Bound WWN** column is not valid (not in xx:xx:xx:xx:xx:xx:xx:xx format) or if you enter a nickname that has not been configured through the Element Manager.

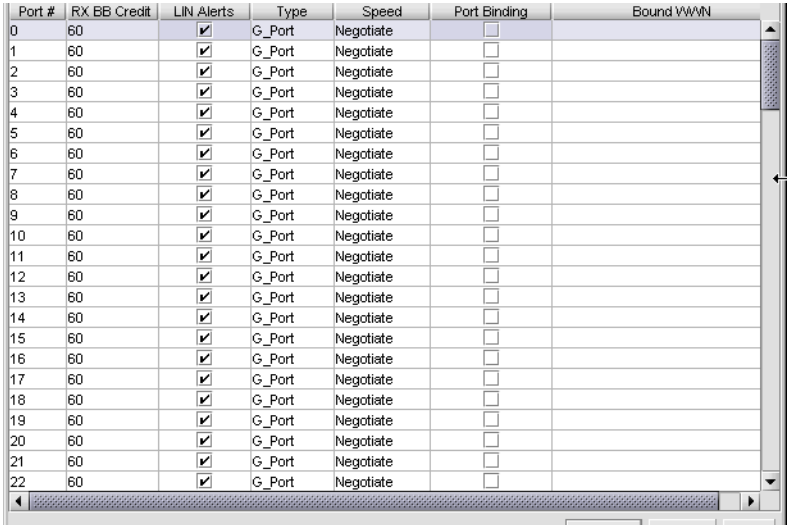
9. To set the data speed for the port, click the **Speed** column for a specific port, and click **2 Gb/sec**, **1 Gb/sec**, or **Negotiate** (2 Gb/sec switch) or 1 **Gb/sec only** (1 Gb/sec switch). Choosing **Negotiate** allows the port and attached device to negotiate the data rate.
10. Use the scroll bar on the right side of the Configure Ports dialog box table to display additional ports that you want to configure.
11. Activate changes and close the dialog box by clicking **Activate**.
12. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

# Configure Ports Procedure (FICON Management Style)

**NOTE:** This procedure applies only to the Edge Switch 2/32. FICON Management Style is not available on the Edge Switch 2/24.

To configure Edge Switch 2/32 ports in FICON management style, use the following steps:

1. Select **Configuration > Ports**. The Configure Ports dialog box appears.



| Port # | RX BB Credit | LIN Alerts | Type | Speed | Port Binding | Bound WWN |
|---|---|---|---|---|---|---|
| 0 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 1 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 2 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 3 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 4 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 5 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 6 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 7 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 8 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 9 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 10 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 11 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 12 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 13 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 14 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 15 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 16 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 17 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 18 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 19 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 20 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 21 | 60 | ☑ | G_Port | Negotiate | ☐ | |
| 22 | 60 | ☑ | G_Port | Negotiate | ☐ | |

**Figure 31** Configure Ports dialog box (FICON Management Style)

Ports are numbered from 0 through 31.

2. Enable or disable extended distance buffering for the port by clicking the check box in the **10-100 km** column. When a check mark displays, extended distance buffering is enabled.
3. If a switch supports BB Credit, the **RX BB Credit** column replaces the **10-100km** column. Use this to set minimum and maximum allowable port BB credit values:
   a. Right-click in the RX-BB Credit column to display the RX BB Credits dialog box as shown in Figure 32:

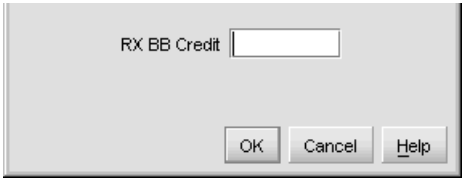



**Figure 32** RX BB Credit dialog box

Set the values as follows:

- For switches without buffer pools, use **Set all...** to set all ports to a single value or **Set all to maximum** which set all ports to a maximum BB credit value.
- For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or select **Distribute**, which evenly distributes the pool buffers among all ports.

**b.** Confirm your changes:

- Clicking **OK** changes the values in the Configure Port dialog box.
- Clicking **Activate** changes the values on the switch.

4. Enable or disable LIN alerts for the port by clicking the check box in the **LIN Alerts** column. When a check mark displays, LIN alerts are enabled.

---

**NOTE:** The factory default for LIN alerts is enabled.

---

5. To bind a device with a specific WWN or nickname to the port, click the **Port Binding** check box to display a check mark. Then enter the WWN or configured nickname for the device into the **Bound WWN** column. The device that you bind to the port will have exclusive connection to that port.

---

**NOTE:** If you have configured Port Binding and click **Activate**, a warning dialog box appears if one or more of the nodes attached to a port does not match the WWN or nickname configured in the **Bound WWN** column. This warning box displays a list of all attached nodes that will be logged off if you continue. If you click **Continue**, these nodes will log off and the port will only attach to the device with the WWN or nickname configured in the **Bound WWN** column.

If you have configured Port Binding and click **Activate**, an error message may display if the format for the WWN entered in the **Bound WWN** column is not valid (not in xx:xx:xx:xx:xx:xx:xx:xx format) or if you enter a nickname that has not been configured through the Element Manager.

---

6. To set the data speed for the port, click the **Speed** column for a specific port, and click **2 Gb/sec**, **1 Gb/sec**, or **Negotiate** (2 Gb/sec switch) or **1 Gb/sec only** (1 Gb/sec switch). Clicking **Negotiate** allows the port and attached device to negotiate the data rate.
7. Use the scroll bar on the right side of the Configure Ports dialog box table to display additional ports that you want to configure.
8. Activate changes and close the dialog box by clicking **Activate**.
9. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

# Configuring port addresses (FICON Management Style)

Use the Configure Address - "Active" dialog box (see Figure 34 on page 98) to create and activate port address configurations.

**NOTE:** This procedure applies only to the Edge Switch 2/32. FICON Management Style is not available on the Edge Switch 2/24.

## Port address parameters

The Configure Addresses - "Active" dialog box contains the following parameters:

- **Addr**—This read-only box lists the port address.
- **Port Name**—This user-defined name is assigned to the address. Up to 24 alphanumeric characters are allowed, including spaces, hyphens and underscores.
- **Blocked**—If the box is checked, the port is blocked. Blocked ports continuously transmit offline sequences (OLSs), but cannot communicate to an attached device. If the box is not checked, the port is unblocked.
- **Port connection array**—This yellow area of the dialog box is a matrix of port addresses that is used to configure connections between port addresses. Each port in the switch has a corresponding port address, which is the physical port number in hexademical format.

  All port addresses for the switch are listed along the top and left side of the matrix. To allow or prohibit connections between two addresses, click the cell at the intersection of vertical and horizontal rows. Right-click the intersecting cell to display a menu of attributes.

  The default state of a cell is an empty cell (square), which represents an allowed connection. The symbol for a prohibited connection is shown in Figure 33. Click a cell to add the prohibited symbol and prohibit connection to that cell.

**Figure 33** Prohibited Port Connection symbol

Move your mouse pointer over the squares in the array to display the corresponding address. Right-click on the array to display the following menu options:

- **Prohibit row**—Prohibits connection between all addresses in a row. In effect, this prohibits connection between a specific address and all other port addresses.
- **Allow row**—Allows connection for all port addresses on a row that are currently prohibited. This allows connection between a port with a specific address and other allowed ports.
- **Prohibit all**—Prohibits connection between all port addresses. In this state, ports in the switch cannot connect with any other port address.
- **Allow all**—This allows a dynamic connection through all port addresses from which connection is currently prohibited. The allowed attribute has the lowest precedence and does not override any other attribute.

- **Block all ports**—Blocks communication between all ports. Ports that are blocked continuously transmit offline sequences (OLSs).
- **Unblock all ports**—Unblocks all port addresses that are currently blocked. This allows communication from all port addresses in the switch.
- **Clear all**—Clears the prohibit and blocked status of all port addresses in the switch.

- **CUP Name**—This user-defined name is assigned to the control unit port (CUP). Up to 24 alphanumeric characters allowed, including spaces, hyphens and underscores. A space character is not allowed as the first character, and the characters are case-sensitive. This is not a required box.
- **Activate**—Click this button to activate the current configuration. A warning displays before the action occurs.
- **Save As**—Click this button to save the current configuration with a name and description. The saved configuration will be stored on the HAFM appliance and in the Address Configuration Library. See "Managing stored address configurations (FICON Management Style)" on page 99 for information on accessing this library.
- **Cancel**—Click this button to cancel the configuration settings and close the dialog box without saving. If you click this button after clicking the **Save As** button, your changes will be saved, and the dialog box will close.

## Configuring port addresses

To configure, save, and activate port addresses, use the following steps:

1. Select **Configure > Addresses > Active**. The Configure Addresses - "Active" dialog box appears, as shown in Figure 34 on page 98.
2. Click a square to either prohibit or allow connections.

△ **CAUTION:** Take extreme care when configuring PDCMs for E_Ports, as mistakes can render paths unusable and cause complex routing problems. These problems can be difficult to detect and sometimes manifest as end-device issues.

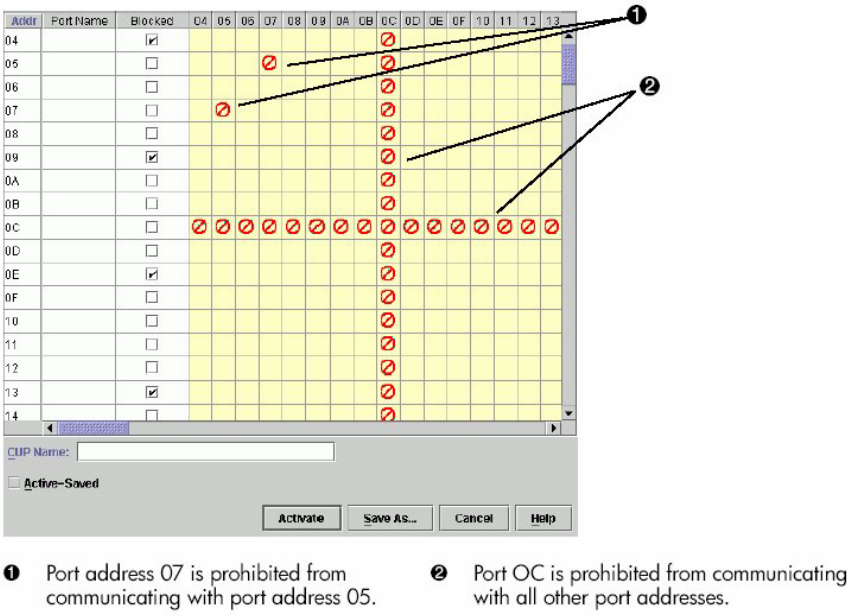



**Figure 34** Configure Addresses - "Active" dialog box

3. Click **Save As** to open the Save Address Configuration As dialog box.
4. Click the **Port Name** box and enter a name.

   Names must be between 1 and 8 characters in length. Valid characters are uppercase A-Z, 0-9, hyphen (-), and underscore (_). The name may not be CON, AUX, COM*n* (*n*=1-49), LPT*n* (*n*=1-39), NUL, or PRN.
5. Click in the **CUP Name** box and enter a name (optional).

   Names must be between 1 and 24 characters. All characters in the ISO Latin - 1 character set are allowed, except for control characters. The space character is not allowed in the first character, and characters are case-sensitive. A CUP name is optional.
6. Click **OK** to save changes and to close the Save Address Configuration As dialog box.
7. In the Configure Addresses - "Active" dialog box, click **Activate** to activate the configuration or click **Cancel** to close without activating.

**NOTE:** If you click **Cancel** after saving, your configuration will still be added to the library without being activated.

# Managing stored address configurations (FICON Management Style)

After address configurations are created through the Configure Addresses - “Active” dialog box, they are saved to the Address Configuration Library. Use this procedure to manage address configurations in the Address Configuration Library.

To manage saved library entries:

1. Select **Configure > Addresses > Stored**. The Address Configuration Library dialog box appears.

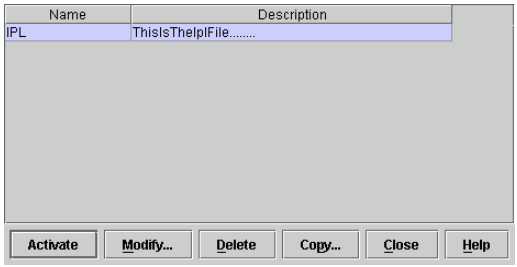



**Figure 35** Address Configuration Library dialog box

2. Choose a configuration entry by clicking on the row. Then use one of the following procedures.
   - To modify a stored configuration:

     Click **Modify**. The Configure Addresses dialog box for the configuration appears. For details on using this dialog box, see ”Configuring port addresses (FICON Management Style)” on page 96.
   - To delete a stored configuration:

     Click **Delete**. A warning displays before deletion.
   - To copy a stored configuration:

     Click **Copy** to copy the configuration and rename/describe it.

     When the Copy Address Configuration dialog box appears, provide a name and description for the configuration. Names must be between 1 and 8 characters in length. Valid characters are uppercase A-Z, 0-9, hyphen (-), and underscore (_). The name may not be CON, AUX, COM*n* (where *n*=1-9), LPT*n* (where *n*=1-9), NUL, or PRN. Descriptions must be between 0 and 24 characters in length. Up to 24 alphanumeric characters are allowed, including spaces, hyphens and underscores. Click **OK** and the configuration is added to the library.
   - Activate a stored configuration

     Click **Activate** to activate the configuration and send it to the switch for immediate use. A warning displays before the action occurs.

---

**NOTE:** If **Active=Saved** is enabled in through the Configure FICON Management Server dialog box (**Configure** menu), this overwrites the current IPL address configuration.

---

3. When finished managing the library, click **Close** to close the dialog box.

# Configure Allow/Prohibit matrix

The Allow/Prohibit matrix option displays two options, Active and Stored. These options display a Configure Allow/Prohibit Matrix window that lets you interact with the element manager while the window is open. You can also minimize, maximize, and close the window from the title bar. Figure 36 shows the Configure Allow/Prohibit dialog box that can be open continuously and updates automatically.

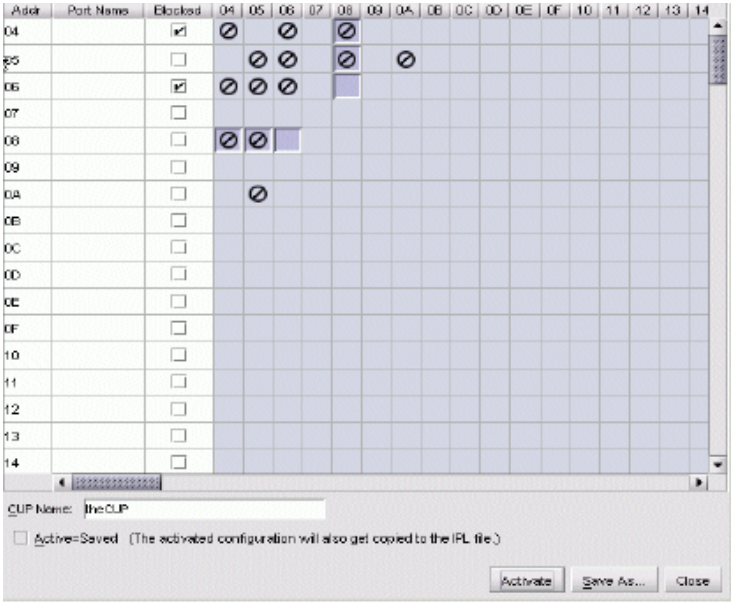



**Figure 36** Configure Allow/Prohibit dialog box

## Accessing Active Configurations

Click **Activate** to display the Allow/Prohibit Matrix Configuration Library dialog box, as shown in Figure 37.

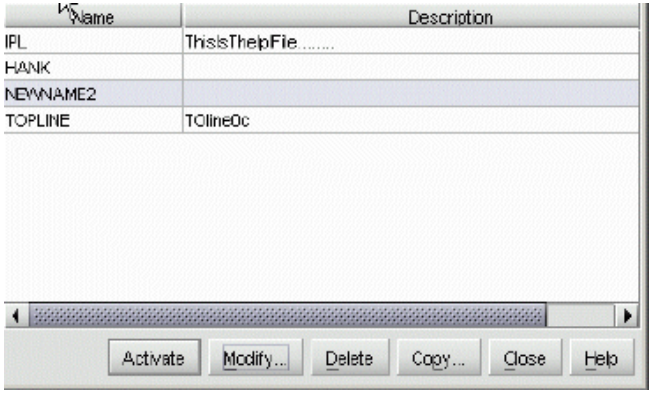



**Figure 37** Configure Allow/Prohibit Matrix Configuration Library dialog box

This dialog box lets you open multiple saved configurations concurrently. Single or multiple configurations can be opened, viewed, edited and saved.

**NOTE:** Create a saved version of the configuration and edit the saved version to minimize the risk of losing current edits. After the edits are completed and saved, then activate the configuration.

## Accessing Stored Configurations

When editing saved configurations, the matrix displays depressed and shaded cells when the matrix cell does not match the saved configuration.

The IPL file is a special saved configuration file. This configuration is used if the switch is in the IPL process. If the Active=Saved option is checked, then the IPL file cannot be edited and saved if Active=Saved. When the IPL is opened, the file dynamically updates if the active configuration changes while the Active=Saved option was enabled.

## Configuring Port Addresses

To configure, save, and activate port addresses, use the following steps:

1. Select **Configure > Allow/Prohibit** to display Configure Allow/Prohibit Matrix - "Active" dialog box.
2. Enter information into the appropriate boxes.
3. Click the squares to either prohibit or allow connections. In the Figure 37, port address 07 is prohibited from communicating with port address 05. Also, Port OC is prohibited from communicating with all other port addresses.

**CAUTION:** Take extreme care when configuring PDCMs for E_Ports as mistakes can render paths unusable and cause complex routing problems. These problems can be difficult to detect and sometimes manifest as end-device issues.

4. Click **Save As** to display the Save Address Configuration As dialog box.
5. Click **Port Name** and enter a name.

   Names must be between 1 and 8 characters in length. Valid characters include uppercase A-Z, 0-9, hyphen (-), and underscore (_). The name cannot be CON, AUX, COM*n* (*n*=1-9), LPT*n* (*n*=1-9), NUL, or PRN.
6. Click **CUP Name** and enter a name.

   Names must be between 1 and 24 characters in length. All characters in the ISO Latin - 1 character set are allowed, except for control characters. The space character is not allowed in the first character and characters are case-sensitive. A CUP name is optional.
7. Click **OK** to save changes and to close the Save Address Configuration As dialog box.
8. In the Configure Allow/Prohibit Matrix - "Active" dialog box, click **Activate** to activate the configuration or click **Cancel** to close without activating.

**NOTE:** If you click **Cancel** after saving, your configuration will still be added to the library without being activated.

## Configuring an SNMP agent

Use the procedures in this section to:

- Configure the SNMP agent that runs on the switch and implements the following MIBs:
  - MIB-II
  - Fabric Element MIB
  - Fibre Alliance (FCMGMT) MIB
  - Switch private MIB

**NOTE:** For complete information on objects defined in MIBs, and steps to download MIB variables to your SNMP workstation, refer to the *HP StorageWorks SNMP reference guide for Directors and Edge Switches*.

- Configure network addresses and community names for up to six SNMP trap recipients.

  An SNMP trap recipient is a network management station that receives messages through SNMP for specific events that occur on the switch.

  To enable or disable authorization trap messages to be sent when unauthorized management stations try to access SNMP information through the HAFM appliance, click the **Enable Authorization Traps** check box. A check mark in the box enables this option.
- Define SNMP community names that SNMP managers use for reading variables.
- Authorize write permissions for writable MIB variables.

**NOTE:** SNMP managers may request, but will not receive, traps and SNMP data through SNMP management stations that are not configured with community names.

To configure SNMP traps and assign community names, use the following steps:

1. Select **Configure > SNMP**. The Configure SNMP dialog box appears, as shown in Figure 38.

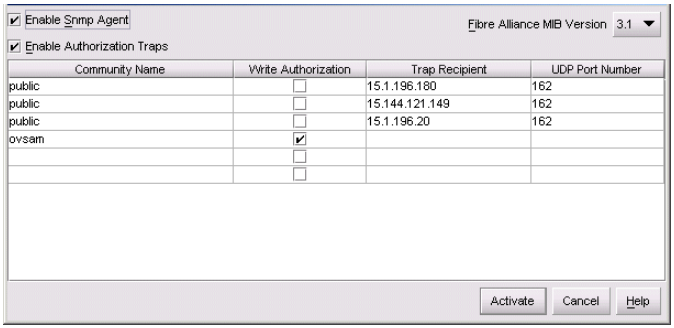



**Figure 38** Configure SNMP dialog box

2. Click **Enable Snmp Agent** to enable or disable an SNMP agent. SNMP agents allow administrators on SNMP management workstations to access product management information using any standard network management tool.
3. Click **Enable Authorization Traps** to enable or disable authorization trap messages to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the switch.
4. Select the Fibre Alliance MIB version supported on the Switch by clicking on the drop-down list in the top right corner of the dialog box. Selections are 3.0 and 3.1.
5. Click a box in the **Community Name** column to select the row. Enter the SNMP community name for the trap recipient. Enter up to 32 characters. This also defines community names from which SNMP managers can read MIB variables from, or write MIB variables to, the switch. See the first note under "Configuring an SNMP agent" on page 102 for more information about MIB variables.
6. Choose the Fibre Alliance MIB version supported on the switch by clicking on the drop-down list in the top right corner of the dialog box. Choices are **3.0** and **3.1**.
7. Click the **Write Authorization** check box to enable write authorization for the community name. A check mark displays in the box to indicate that write authorization is enabled.
8. Enter the IP address for a trap recipient (SNMP management station) by clicking in the **Trap Recipient** column and entering an IP address.

---

**NOTE:** In most cases, step 9 is not necessary. If you do not wish to override the default UDP number, skip to step 10.

---

9. Enter user datagram protocol (UDP) port numbers in the **UDP Port Number** column. You can override the default UDP port number of 162 with any legal UDP port number (1 to 65535).
10. Click **Activate** to activate the data and close the dialog box.

    The SNMP configuration is stored in NV-RAM on the switch.

11. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

## Configuring Open Systems management server

Edge Switch 2/32 only. For complete procedures on configuring this optional feature, see "Open Systems Management Server" on page 151.

## Configuring FICON management server

Edge Switch 2/32 only. For complete procedures on configuring this optional feature, see "Configuring the FICON Management Server" on page 149.

## Configuring a feature key

Feature keys verify ownership of the Element Manager and optional features that can be purchased for the Element Manager. The feature key, which is encoded with a switch's serial number, can only be configured on the switch to which it is assigned.

A feature key is a string of alphanumeric characters consisting of both uppercase and lowercase characters. The following is an example of a feature key format: XxXx-XXxX-xxXX-xX.

**NOTE:** The total number of characters may vary. The key is case sensitive and must be entered exactly, including the dashes.

**NOTE:** You can configure a feature key with the switch online. However, if a current feature is disabled by activating a new feature key, take the switch offline before enabling the new feature key.

The feature key, which is encoded with a switch's serial number, can only be configured on the switch to which it is assigned.

To enable an optional feature on the switch, enter the feature key into the New Feature Key dialog box. Display this dialog box by clicking **Configure > Feature**.

**NOTE:** For detailed descriptions of features that you can enable using the Configure Feature Key dialog box, see "Optional features" on page 143.

To configure a feature key, use the following steps:

1. Set the switch offline using the Set Online State dialog box. For help, see "Setting online state" on page 136.

**NOTE:** You do not need to set the switch offline to install a feature key, unless some feature functionality is being removed. If you are adding features or ports, you do not need to take the switch offline.

2. Select **Configure > Features**. The Configure Feature Key dialog box appears.

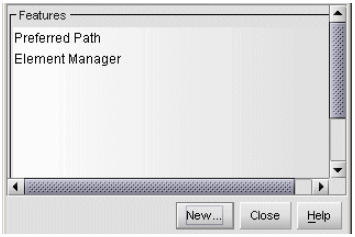



**Figure 39** Configure Feature Key dialog box

3. Click **New** to add a new feature key.
4. In the New Feature Key dialog box, enter the switch's feature key and click **OK**.
   - Feature keys are only valid for a switch with a specific serial number. They cannot be interchanged between switches. If an error stating `Invalid serial number` displays, verify that you have entered the feature key that was assigned to the switch. To verify, check the serial number of the switch through the Switch Properties dialog box and compare it to the serial number listed in the documentation provided with your feature key. See"Displaying switch information" on page 54 for instructions on displaying the Switch Properties dialog box.
   - The feature key is a string of alphanumeric characters with dashes. The key is case-sensitive, so enter the key exactly as printed in the documentation that you received for the feature. If an error stating `Invalid feature key` displays, verify that you have entered the feature key correctly.

     The Enable Feature Key dialog box (Figure 40) displays with a warning, stating that this action will override the current set of features on the switch. The list in the left column of the dialog box is a list of features that are active on the switch.

The list on the right is a set of features that come with the new feature key. All of the features that are active are included in the new feature list.

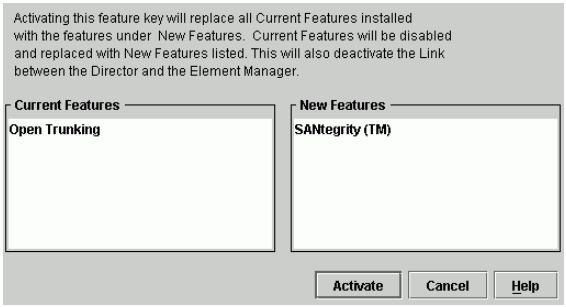



**Figure 40** Enable Feature Key dialog box

5. Click **Activate** to activate the new feature key.

   An IPL will occur, during which the Ethernet connection between the HAFM appliance and switch is momentarily interrupted. This will not disrupt Fibre Channel traffic.

**NOTE:** f you click **Activate**, all current features will be replaced with new features. That is, if there are features shown in the current list that are not shown in the new list, then those features will be removed from the switch.

6. When you are finished configuring the switch, you can back up the configuration data. For more information, see "Backing up and restoring configuration data" on page 117.

## No Feature Key dialog box

If you attempt to access a feature for which a feature key was not enabled, a No Feature Key dialog box appears.

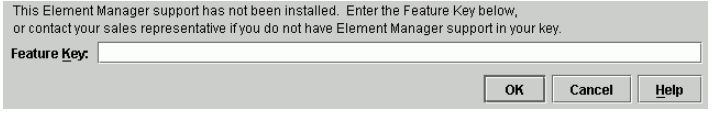



**Figure 41** No Feature Key dialog box

At this point, you must enter the Element Manager feature key. After you enter a valid feature key, the Enable Feature Key dialog box appears.

Click **Activate** on the Enable Feature Key dialog box to activate the new feature key. An IPL will occur, during which the Ethernet connection between the HAFM appliance and director is momentarily interrupted. This will not disrupt Fibre Channel traffic.

**NOTE:** If you click **Activate**, all current features will be replaced with new features. That is, if there are features shown in the current list that are not shown in the new list, then those features will be removed from the switch or director.

Because the switch or director is placed offline when you activate the Element Manager feature key, the Element Manager will not launch until it comes back online and you either:

- Right-click the switch or director and click **Element Manager**.
- Choose the switch or director and click the Launch Element Manager icon on the tool bar.

# Configuring date and time

Use the procedures in this section to display and change the date and time set on the switch. You must set the current date and time on the switch using this dialog box so that the correct time stamps display in the Event Log, Audit Log, Hardware Log, Link Incident Log, and Threshold Alerts Log.

Set the switch date and time using the following steps:

1. Select **Configure > Date/Time**. The Configure Date and Time dialog box appears, as shown in Figure 42.

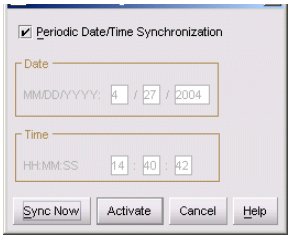



**Figure 42** Configure Date and Time dialog box

2. You can set the switch date and time manually or you can set it for periodic synchronization with the HAFM appliance. For specific instructions, see the following sections:
   - "Setting date and time manually"
   - "Synchronizing date and time"

## Setting date and time manually

Use these steps to set the switch date and time manually.

1. At the Configure Date and Time dialog box, click the **Periodic Date/Time Synchronization** check box to deselect the option (no check mark in the box). The grayed-out **Date** and **Time** boxes activate, as shown in Figure 43.

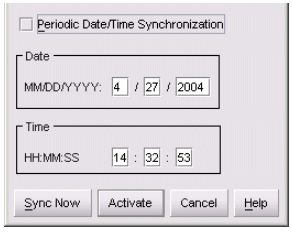



**Figure 43** Configure Date and Time dialog box (manual options)

2. Click the **Date** box that require change, and type numbers in the following ranges:
   Month (MM): 1 through 12
   Day (DD): 1 through 31
   Year (YYYY): greater than 1980
3. Click the **Time** box that require change, and type numbers in the following ranges:
   Hour (HH): 0 through 23
   Minute (MM): 0 through 59
   Second (SS): 0 through 59
4. Click **Activate** to set the director date and time, and close the Configure Date and Time dialog box.

## Synchronizing date and time

Use these steps to set the director to periodically synchronize date and time with HAFM.

1. At the Configure Date and Time dialog box, click the **Periodic Date/Time Synchronization** check box. The **Date** and **Time** boxes are grayed-out and not selectable, as shown in Figure 44.

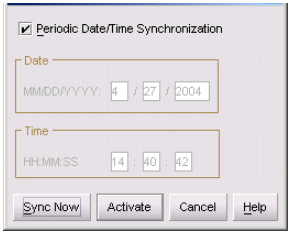



**Figure 44** Configure Date and Time dialog box (periodic synchronization options)

2. You can choose one of the following:
   - Click **Activate** to enable synchronization and close the Configure Date and Time dialog box. The switch date and time synchronize with the HAFM appliance date and time at the next update period (at least once daily) and Daylight Savings Time automatically updates.
   - Click **Sync Now** to synchronize the switch and HAFM appliance immediately. The Date and Time Synced dialog box appears.
   - Click **OK**.
   - In the Configure Date and Time dialog box, click **Activate** to enable synchronization and close the Configure Date and Time dialog box.

# Configuring threshold alerts

A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific switch ports or port types, (E_Ports, F_Ports, or FL_Ports).

You are notified of a threshold alert by:

- An attention indicator (yellow triangle) that displays on the port in the Hardware View.
- An attention indicator (yellow triangle) that displays in the **Alert** column of the Port List View.
- An attention indicator (yellow triangle) that displays by the **Threshold Alerts** box in the Port Properties dialog box.
- Detailed threshold alert data recorded in the Threshold Alert Log.

## Threshold alert configuration parameters

Use the **Threshold Alerts** option on the **Configure** menu to configure the following:

- Name for the alert.
- Type of threshold for the alert (Rx, Tx, or either).
- Active or inactive state of the alert.
- Threshold criteria:
  - Percent traffic capacity utilized. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value. For example, the value of 50 means that the port's threshold is reached when throughput is 50% of capacity.
  - Time interval during which throughput is measured and alert notification can occur.
  - The maximum cumulative time that the throughput percentage can be exceeded during the set time interval before an alert is generated.
- Ports for which you are configuring threshold alerts.

You can configure up to 16 alerts, and any number of alerts can be active at one time.

Use the following procedures to create a new threshold alert, or to modify, activate, deactivate, or delete an alert.

## Creating new alerts

Use the following steps to create a new threshold alert configuration:

1. Select **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box appears, as shown in Figure 45.

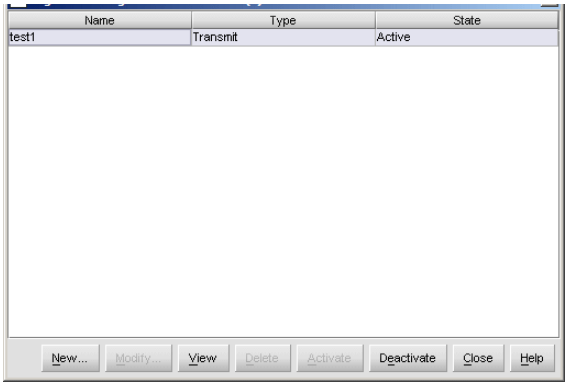



**Figure 45** Configure Threshold Alerts dialog box

If alerts are configured, they will display in table format, showing the name of the alert, type of alert (Rx, Tx, or Rx or Tx), and alert state (inactive or active).

2. Click **New**. The New Threshold Alert dialog box appears, as shown in Figure 46.

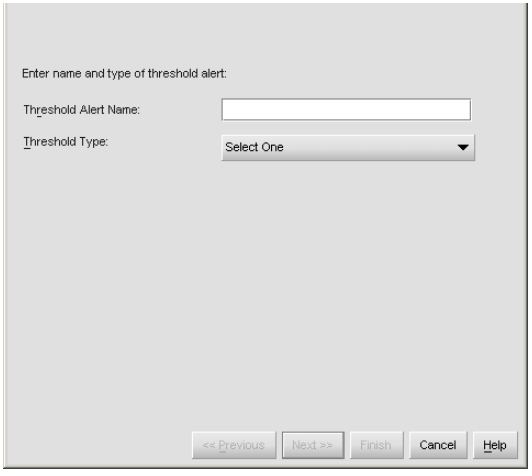



**Figure 46** New Threshold Alerts dialog box - first screen

3. Enter a name from 1 to 64 characters in length. All characters in the ISO Latin-1 character set, excluding control characters, are allowed.

4. Click one of the following on the drop-down list in the **Name** box:
   - **Transmit**. An alert will occur if the threshold set for transmit throughput is reached.
   - **Receive**. An alert will occur if the threshold set for receive throughput is reached.
   - **Receive and Transmit**. An alert will occur if the threshold set for either receive or transmit throughput is reached.
5. Click **Next**. A new screen displays with additional parameters, as shown in Figure 47 on page 111. The name configured for the alert displays at the top of the screen.
   (Click **Previous** to return to the previous screen.)

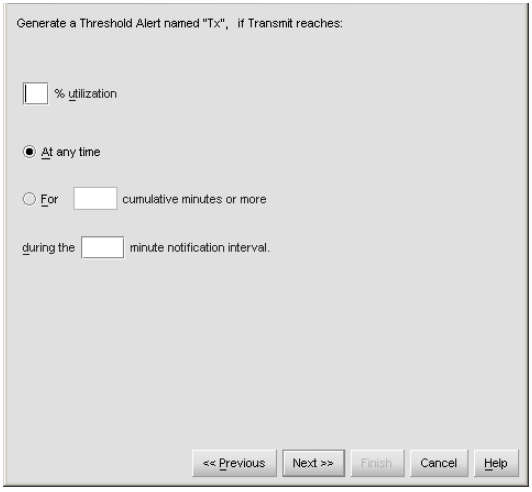



**Figure 47** New Threshold Alerts dialog box - second screen

6. Enter a percentage from 1 through 100 for **% utilization**. When throughput reaches this percentage of port capacity, a threshold alert will occur.
7. Enter the amount of cumulative minutes in which the **% utilization** should exist during the notification interval before an alert is generated. You can also click **At any time** if you want an alert to occur whenever the set **% utilization** is reached. The valid range is 1 to the interval set in step 8.
8. Enter the interval in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.

9. Click **Next**. A new screen displays for choosing ports for the alerts, as shown in Figure 48.

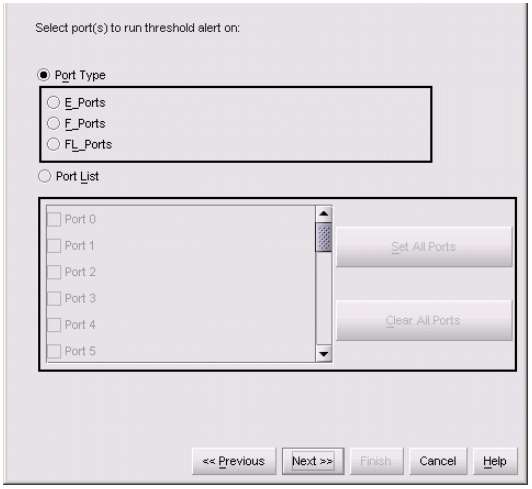



**Figure 48** New Threshold Alerts dialog box - third screen (Edge Switch 2/24)

10. Click either **Port Type** or **Port List**.
    - If you click **Port Type**, clicking either E_Ports, F_Ports, or FL_Ports will cause this alert to generate for all ports configured as E_Ports, F_Ports, or FL_Ports respectively.
    - If you click **Port List**, you can choose individual ports by clicking the check box by each port number or you can click **Set All Ports**. Clicking **Set All Ports** places a check mark by each port number. Clicking **Clear All Ports** will clear the check marks by each port number.
11. Click **Next**. A final screen displays a summary of your alert configuration, as shown in Figure 49.

To make any changes, move backwards and forwards through the configuration screens by clicking **Previous** and **Next**.

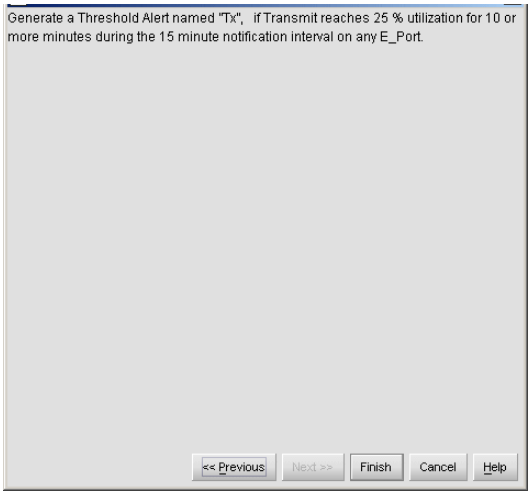



**Figure 49** New Threshold Alerts dialog box - summary screen

12. Click **Finish**. The Configure Threshold Alerts dialog box appears, listing the name, type, and state of the alerts that you just configured.
13. At this point, the alerts are not active. To activate the alerts, click the alert information that displays in the **Configure Threshold Alerts** table and click **Activate** as shown in Figure 50.

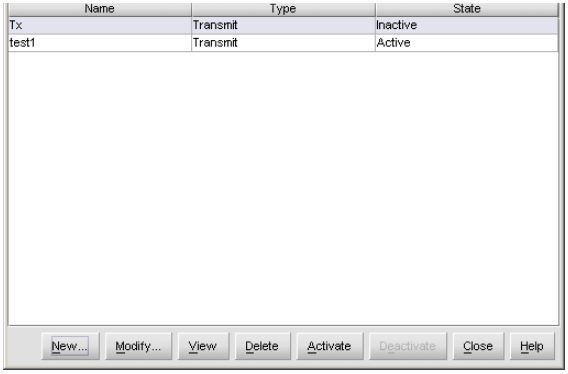



**Figure 50** Configure Threshold Alerts dialog box - alerts activated

## Modifying alerts

Use the following steps to modify an existing threshold alert configuration.

1. Select **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box appears.
2. Select the alert that you want to modify by clicking the alert information in the table.
3. If the alert is active, click **Deactivate**, then choose the alert information in the table again.
4. Click **Modify**. An initial Modify Threshold screen displays where you can change the threshold type.
5. Select a threshold type from the drop-down list.
6. Click **Next** when you are done. A Modify Threshold screen displays where you can change the % utilization, cumulative minutes for the threshold to occur before notification, and the time interval for measuring throughput and for alert notification.
7. Make appropriate changes, then continue through the Modify Threshold screens, making changes as necessary, until the summary screen displays the alert configuration.
8. Perform either of the following steps:
   - If you need to change any parameters, click **Previous** and **Next** to display the desired Modify Threshold screen.
   - Click **Finish** when you are done.

If you want to view the details of the modified threshold alert, follow the procedures in "Viewing alerts" on page 115.

## Activating or deactivating alerts

Use the following steps to activate or deactivate existing threshold alerts. In the active state, notifications are generated for the alert. In the inactive state, notifications do not occur.

1. Select **Configure > Threshold Alerts** from the menu.

   The Configure Threshold Alerts dialog box appears. The port's current state, `Inactive` or `Active`, is listed in the **State** column.
2. To change the state, select the alert information in the table.
3. If the alert is active, click **Deactivate** to change to the inactive state. If the alert is inactive, click **Activate** to change to the active state.

## Viewing alerts

Use the following steps to view existing threshold alerts.

1. Select **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box appears.
2. Select the alert that you want to view by selecting the alert information in the table.
3. Click **View**. The View Threshold Alerts dialog box appears, describing the threshold alert and the ports to which the alert has been applied.

## Deleting alerts

Use the following steps to delete existing threshold alerts.

1. Select **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box appears.
2. Select the alert that you want to delete by selecting the alert information in the table.
3. Click **Delete**. A message asking you to confirm the deletion displays.
4. Click **Yes**. The alert is removed from the dialog box.

# Configuring Open Trunking

This option is only available if the optional Open Trunking feature is installed and the firmware is version 06.01.00 or higher. Choosing this option opens the Configure Open Trunking dialog box. For details on enabling Open Trunking and configuring such parameters as congestion thresholds for ports, event notification options, and the Low BB Credit Threshold, see "Open Trunking" on page 158.

# Exporting the Configuration Report

The Export Configuration Report dialog box enables you to create an ASCII file of all saved configuration data in the switch's NV_RAM. The file is saved to your hard drive or a diskette. Use any program that can read ASCII text to import this file for viewing or printing.

The Export Configuration Report dialog box is available on the Configuration menu.

**NOTE:** This file cannot be used to set configuration parameters through the Element Manager.

## Configuration Report parameters

Data in the file includes:

- **Product identification**—Data input into the Configure Identification dialog box.
- **Operating parameters**—Data input into the Operating Parameters (Switch and Fabric) dialog box.
- **Port parameters**—Data input into the Configure Ports dialog box.
- **SNMP parameters**—Data input into the Configure SNMP dialog box.
- **Active zoning configuration**—Specifies the active zone and zone members, if set, and whether the default zone is enabled or disabled.

To export a configuration report:

1. Select **Configure > Export Configuration Report**.
   The Export Configuration Report dialog box appears.

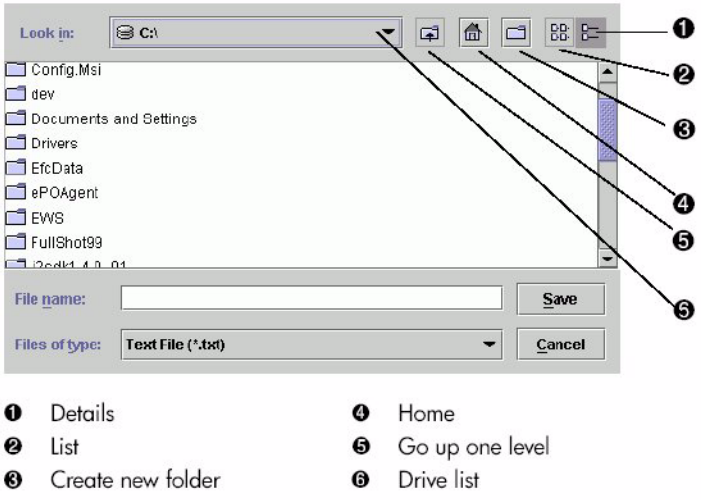



**Figure 51** Export Configuration dialog box

2. Select the folder where you want to save the file.
3. Enter a file name and extension in the **File name** box.
4. Click **Save**. The file saves to the specified folder as an ASCII text file.

# Enabling Embedded Web Server

Use the following steps to enable EWS:

1. At the Hardware View page, select **Configure > Enable Web Server**. Selecting **Enable Web Server** automatically places a check mark in the check box.
2. Click **Enable Web Server** again to remove the check mark and disable the EWS interface. When disabled, remote users cannot access the interface.

For complete procedures on using EWS, refer to *HP StorageWorks Embedded Web Server user guide*.

# Enabling Telnet

1. At the Hardware View, select **Configure > Enable Telnet**. Clicking **Enable Telnet** automatically places a check mark in the check box.
2. Click **Enable Telnet** again to remove the check mark and disable Telnet access. When disabled, remote users cannot access the director through Telnet.

# Enabling Alternate Control Prohibited

You can display Alternate Control Prohibited (ACP) in the Configure menu by selecting the check box to set the ACP on or off. When the ACP is checked, alternate control prohibited is on and alternate managers cannot change FICON switch connectivity parameters.

These parameters include all configuration changes including, but not limited to blocking ports, beaconing ports, clearing, LINs, CTP switch over and so on. The alternate managers include CLI, EWS, SNMP, but do not include the host via inband management.

The ACP setting is only controlled by the HAFM and cannot be changed by Host Programming. Select the option again to remove the check mark and disable Alternate Control Prohibited.

---

**NOTE:** The Alternate Control Prohibited checkbox is only visible for switches that support ACP. Prior to sending the ACP setting to the switch, confirm the warning dialog box that displays that states you are about to disable alternate configuration control.

---

# Backing up and restoring configuration data

You can back up the NV-RAM configuration, which includes all of the data you input through instructions in this chapter, using the **Backup and Restore Configuration** option. This option is available through the **Maintenance** menu. Choosing this option backs up the configuration data to a file on the HAFM appliance hard drive. The restore function writes this data back to NV-RAM on the switch. Using the restore function overwrites the existing configuration. For more information, see "Backing up and restoring configuration" on page 138.

In addition to the **Backup and Restore Configuration** option, the backup application automatically backs up configuration and other critical data from the HAFM appliance. As long as backup media remains in the backup drive of the HAFM appliance, data is written to the backup media whenever the directory contents change or you reboot the HAFM appliance. For more information, see "Backing up and restoring Element Manager data" on page 42.

**NOTE:** We do not recommend changing the default backup settings.

**CAUTION:** To ensure trouble-free backups, it is imperative that you leave the backup media in the drive at all times. Removing the media during a backup or restore can corrupt the database on the media. When data is being written to or read from the backup drive, the CD-RW drive write LED flashes. Make sure this LED is not flashing before you remove the media.

# 4 Using logs

This chapter describes the Edge Switch logs that you can access through the Logs menu on the Element Manager menu bar:

# Log options and functions

The Audit, Event, Hardware, Link Incident, and Threshold Alert logs store up to 1000 entries each. The most recent entry appears at the top of the log. After 1000 entries are stored, new entries overwrite the oldest entries.

## Using buttons

The following buttons work the same way for all logs:

- **Close**—Clicking **Close** closes the log and displays the switch Element Manager window.
- **Refresh**—Clicking **Refresh** reads the current data and refreshes the screen with the new display.
- **Clear**—Clicking **Clear** clears all entries in the log for all users. A Warning dialog box appears requesting confirmation that you want to clear all entries in the log. (**Clear** is not valid for the Open Trunking Log. For more information, see "Open Trunking log" on page 161.)
- **Export**—Clicking **Export** on a log window displays the Save dialog box shown in Figure 52 on page 121. Click the **Home** icon to return to the files in your home directory. The folders that are shown in the display area of the Save dialog box after clicking the **Home** icon are those that are stored in your home directory. If you choose, you may create a folder for your home directory and save the file there.

  To save a log file in American Standard Code for Information Interchange (ASCII) format to a location on your system's hard drive or to a diskette, use the following steps. You can open this file in any program that can read ASCII files for viewing or printing.

## Saving a log file

To save a log to a file:

1. Click **Export** on the log window to display the Save dialog box. This dialog box contains the controls shown in Figure 52.

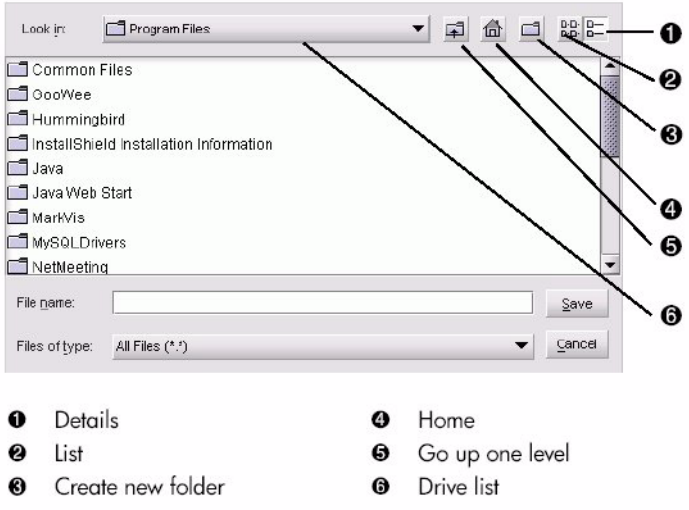



**Figure 52** Save dialog box—log windows

2. In the Save dialog box, select the folder where you want to save the file.
3. Enter a file name and extension in the **File name** box.
4. Click **Save**.

The file saves to the specified folder as an ASCII text file.

## Expanding columns

Expand columns in logs by placing the mouse pointer over the line between column headings until a double arrow appears. Then, click and drag the line to widen the column as necessary.

## Sorting entries

Sort log entries in columns by clicking a column heading. A down arrow indicates the items in the column are being sorted alphabetically in descending order. An up arrow indicates the items are being sorted in ascending order. Click once to sort. Click again to reverse the sort.

# Audit log

The Audit Log displays a history of all configuration changes applied to the switch from any source, such as Element Manager, SNMP management stations, Web server interface, host, or another switch. To open the Audit Log, select **Logs > Audit Log**.

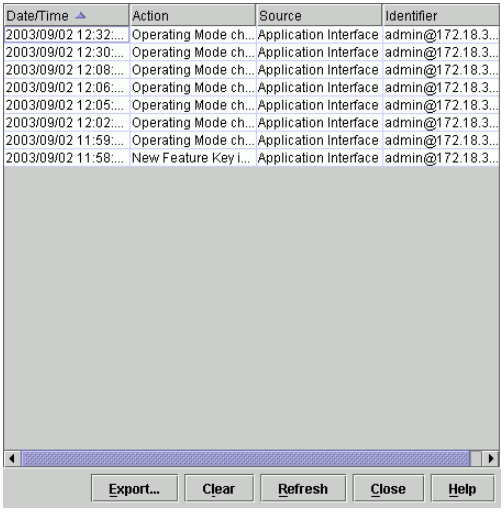



**Figure 53** Audit Log

The following describes each column in the Audit Log:

- **Date/Time**—Displays the date and time of a change on the switch.

  Some actions, such as backing up configuration data and enabling automatic date/time synchronization, are performed only by the HAFM appliance without switch interaction. These actions are indicated by the string, `Application Interface`, following the audit log's stamp of the appliance's date and time (see Figure 53). If the string `Application Interface` is not displayed, the time stamp is from the switch.
- **Action**—Describes the user action that caused the configuration change, such as offline status, port name change, or change of address.
- **Source**—Identifies the user making the change through the switch Element Manager and the IP or DNS host name address of the remote user's workstation.
  - Maintenance Port—Change was made by a user connected to the maintenance port.
  - Application Interface—Change was made by an Element Manager user.
  - SNMP—Change was made by a remote SNMP management station.
  - Fabric—Change was initiated by another switch in the fabric that is not managed by this HAFM appliance.
  - Embedded Web server—Change was made by a user through the EWS interface.
  - Fibre Channel Host—Change was made inband by a Fibre Channel host through the Open Systems Management Server.
  - Telnet—Change was made through a telnet connection by the Command Line Interface.

- **Identifier**—Identifies the user making the change according to the source:
  - Maintenance Port—No entry appears.
  - HAFM—Includes `user@address`, where `user` is the Element Manager user name and `address` is the network address of the workstation (remote user workstation or HAFM appliance).
  - SNMP—Contains the network address of the SNMP management station.
  - Fabric—No entry appears.
  - Web Server—The Identifier column contains `user@address`. The `user` is the Web server user name and `address` is the network address of the Web user.
  - Fibre Channel Host—No entry appears.
  - Telnet—Change was made through a telnet connection.

# Event log

The Event Log provides a record of significant events that have occurred on the switch, such as hardware failures, degraded operation, and port problems. To open the Event Log, select **Logs > Event Log**.

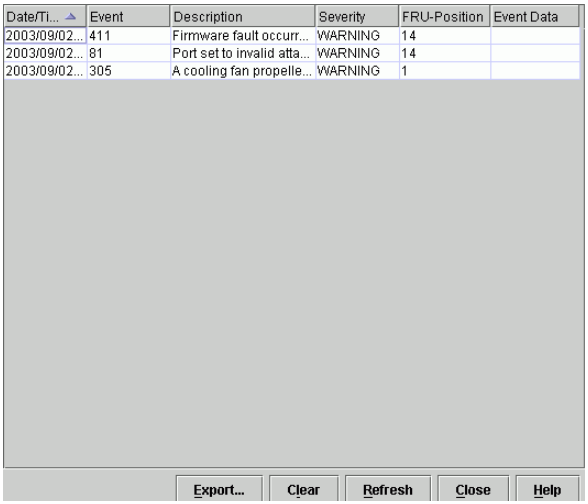



**Figure 54** Event Log

All detected firmware faults and hardware failures are sent to the HAFM appliance for recording in the Event Log. The log provides a maximum of 1000 log entries before it wraps and overwrites the oldest entries. For detailed information on event data and problem resolution, refer to the appropriate service manual for your Edge Switch.

Each log entry includes the following:

- **Date/Time**—The date and time of the event on the switch.

- **Event**—Events are identified by a unique code. Table 5 lists the event codes and their corresponding event types.

**Table 5** Event codes

| Event Codes | Corresponding Event Type |
|---|---|
| 000 - 199 | System events |
| 200 - 299 | Power supply events |
| 300 - 399 | Fan module events |
| 400 - 499 | CTP events |
| 500 - 599 | Port events |
| 800-899 | Thermal events |

- **Description**—A short description of the event.
- **Severity**—The following classifications of severity identify the importance of the event:
  - 0=Informational
  - 2=Warning
  - 3=Fatal
  - 4=Fatal, not operational

  The FRU involved in the event, and the slot position in the chassis, relative to identical FRUs installed.
- **Event Data**—Up to 32 bytes of supplementary information for the event in hexadecimal format. For detailed information on event data and problem resolution, refer to the event code tables appendix in the *HP StorageWorks Edge Switch 2/24 service guide* or the *HP StorageWorks Edge Switch 2/32 service guide*.

# Hardware log

The Hardware Log displays information about box replaceable units (FRUs) inserted and removed from the switch. To open the Hardware Log, select **Logs > Hardware Log**.

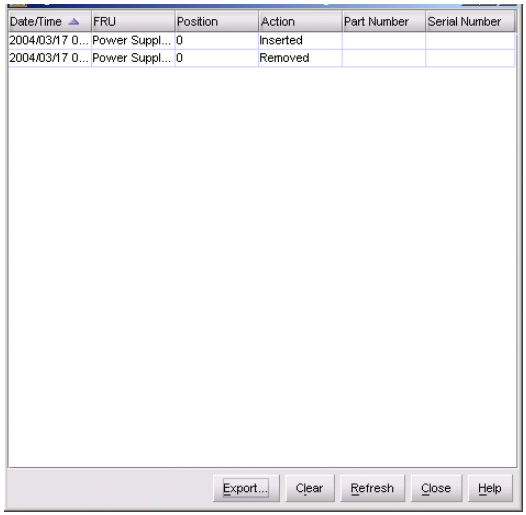



**Figure 55** Hardware Log

Each log entry includes the following:

- **Date/Time**—Date and time of the insertion or removal of the FRU.
- **FRU**—The name of the inserted or removed FRU:
  - PWR—Power supply/fan module
  - SFP—SFP transceiver.
  - CTP— CTP card. Note: The CTP is not an FRU.
- **Position**—Slot position in the chassis relative to identical components installed.
- **Action**—Inserted or removed.
- **Part Number**—Part number of the component.
- **Serial Number**—Serial number of the component.

# Link Incident log

The Link Incident Log displays most recent 1000 link incidents, the date each incident occurred, the time it occurred, and the port where it took place. To open the Link Incident log, select **Logs > Incident Log**.

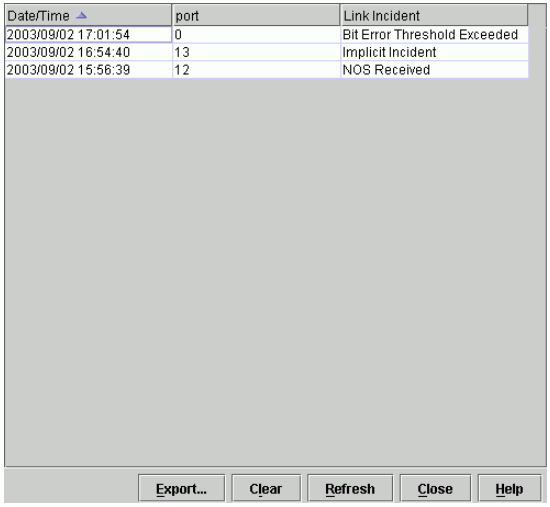


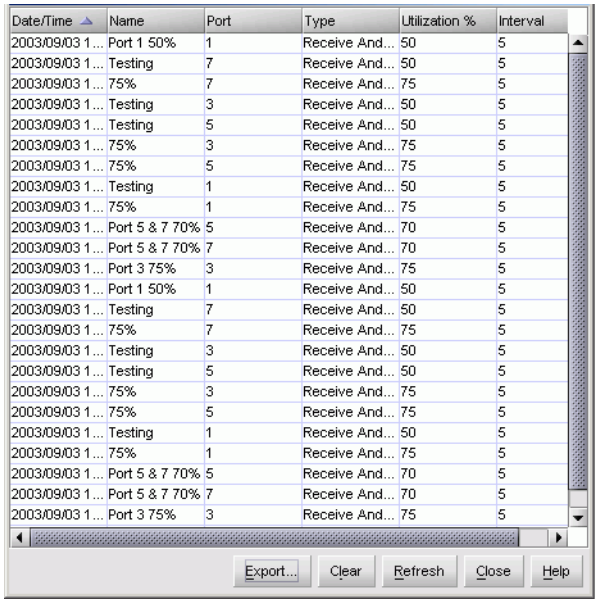

**Figure 56** Link Incident Log

Each log entry contains:

- **Date/Time**—The date and time of the incident.
- **Port**—The number of the port on which the incident occurred.
- **Link Incident**—A short description of the incident. The following events may cause a link incident to be written to the log.
  - Implicit incident—The attached node has detected a condition that may cause problems on the link.
  - Bit-error threshold exceeded—The number of code violation errors has exceeded the threshold.
  - Loss-of-signal or Loss-of-synchronization—Loss-of-signal occurs when a cable is unplugged from an attached node. Loss-of-synchronization occurs when a condition has persisted for longer than the resource allocation time out value (R_A_TOV).
  - Not-operational (NOS) primitive sequence received—A NOS was recognized.
  - Primitive sequence timeout:
  - Link reset protocol timeout occurred.
  - Timeout occurred for an appropriate response while in NOS receive state, and after NOS is no longer recognized.
  - Invalid primitive sequence received for the current link state—Either a link reset or a link reset response primitive sequence was recognized while waiting for the offline sequence.

# Threshold alert log

This log provides details of threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert, as configured through the **Threshold Alerts** option under the **Configure** menu. To open the Threshold alert log, select **Logs > Threshold Alert Log**.



| Date/Time | Name | Port | Type | Utilization % | Interval |
|---|---|---|---|---|---|
| 2003/09/03 1... | Port 1 50% | 1 | Receive And... | 50 | 5 |
| 2003/09/03 1... | Testing | 7 | Receive And... | 50 | 5 |
| 2003/09/03 1... | 75% | 7 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Testing | 3 | Receive And... | 50 | 5 |
| 2003/09/03 1... | Testing | 5 | Receive And... | 50 | 5 |
| 2003/09/03 1... | 75% | 3 | Receive And... | 75 | 5 |
| 2003/09/03 1... | 75% | 5 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Testing | 1 | Receive And... | 50 | 5 |
| 2003/09/03 1... | 75% | 1 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Port 5 & 7 70% | 5 | Receive And... | 70 | 5 |
| 2003/09/03 1... | Port 5 & 7 70% | 7 | Receive And... | 70 | 5 |
| 2003/09/03 1... | Port 3 75% | 3 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Port 1 50% | 1 | Receive And... | 50 | 5 |
| 2003/09/03 1... | Testing | 7 | Receive And... | 50 | 5 |
| 2003/09/03 1... | 75% | 7 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Testing | 3 | Receive And... | 50 | 5 |
| 2003/09/03 1... | Testing | 5 | Receive And... | 50 | 5 |
| 2003/09/03 1... | 75% | 3 | Receive And... | 75 | 5 |
| 2003/09/03 1... | 75% | 5 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Testing | 1 | Receive And... | 50 | 5 |
| 2003/09/03 1... | 75% | 1 | Receive And... | 75 | 5 |
| 2003/09/03 1... | Port 5 & 7 70% | 5 | Receive And... | 70 | 5 |
| 2003/09/03 1... | Port 5 & 7 70% | 7 | Receive And... | 70 | 5 |
| 2003/09/03 1... | Port 3 75% | 3 | Receive And... | 75 | 5 |

Export... Clear Refresh Close Help

**Figure 57** Threshold Alert Log

- **Date/Time**—Date and time stamp for when the alert occurred.
- **Name**—Name for the alert, as configured through the Configure Threshold Alerts dialog box.
- **Port**—Port number where the alert occurred.
- **Type**—The type of alert: transmit (Tx) or receive (Rx).
- **Utilization**—Percent usage of traffic capacity. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value and is configured through the Configure Threshold Alerts dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25% of the port's capacity.
- **Interval**—The time interval during which the throughput is measured and an alert can generate. This is set through the Configure Threshold Alerts dialog box.

# Open Trunking log

The Open Trunking log displays only if the optional Open Trunking feature is installed. For details, see"Open Trunking log" on page 161.

# Security log

The Security log includes information about security events, as shown in Figure 58.

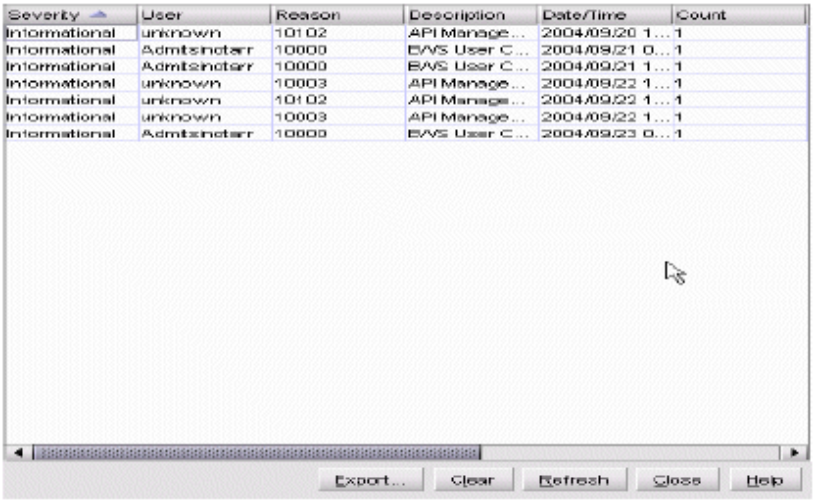



**Figure 58** Security log

The Security log displays the following information:

- **Severity**—The severity level of the event, informational, warning, and fatal.
- **User**—The user associated with the event.
- **Reason**—The reason code for caused the failure.
- **Description**—The security event category and includes the description that lists more details of the event and the IP address of the product.
- **Date and Time**—The date and time that the event occurred. The format is *yyyy/mm/dd hh:mm:ss:tt*. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Count**—The number of times that the same event occurs.
- **Category**—The category.
- **IP**—The IP address.
- **Role**—The role of the user.
- **Interface**—The interface.

# Embedded Port log (Advanced log)

This log provides a detailed history log of all traffic passing through the embedded port. The Embedded Port (EP) of the Switch is a single physical FC port within the hardware architecture that is used to communicate FC frames between devices attached to the external ports and the embedded firmware's FC services software, based on the use of well-known Fibre Channel addresses. This is similar to the function of the Control Unit Port (CUP) in FICON architecture. The CUP is implemented via the EP for FICON traffic. The Embedded Port Log will log all FC frame traffic directed to the switch (EP), including discards, frames not routed, and traffic designated for the EP (inband traffic), as shown in Figure 59.

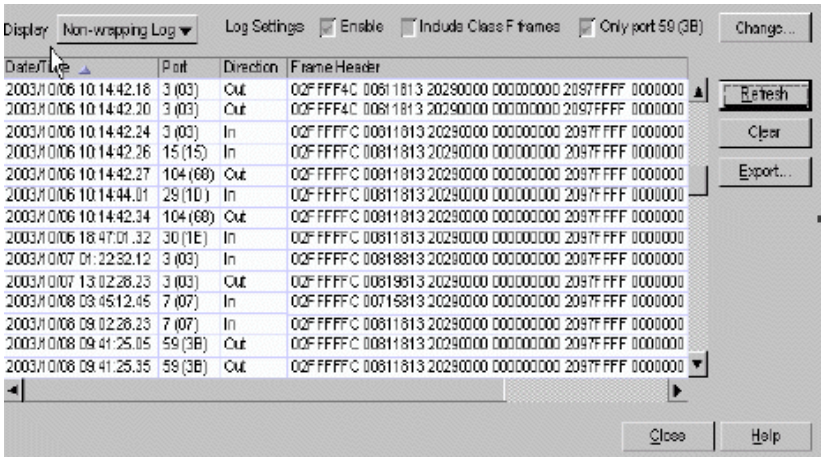



**Figure 59** Embedded Port log (FICON style display mode)

- **Non-wrapping Log or Wrapping Log**—From the submenu, select Non-wrapping log or Wrapping log, Wrapping log is the default.
- **Log Settings**— Displays the current settings of the log options configured on the Switch. These settings affect how log data is captured and stored on the Switch, not just what is displayed in the dialog box. For example, if the Include Class F Frames is turned off or unchecked, Class F frames are not captured or stored in the log on the Switch and are not accessible from this log. To change these options, click the Change... button. For information, Change button-130
- **Date and Time**—The date and time that the event occurred. The format is *yyyy/mm/dd hh:mm:ss:tt*. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Port**—The decimal receive port number on the local Switch associated with the flow that was rerouted. When FICON style is on, the hexadecimal equivalent of the port number appears in parentheses. When FICON style is off, only the decimal value is shown and there is no value in the parenthesis.
- **Direction**—**In** or **Out** indicates the direction of the frame in reference to the embedded port and is related to the port number. For example, if **In** appears, then the frame is coming into the embedded port from the port number specified in the **Port** box.

- **Frame Header**—The Fibre Channel Frame Header string. This header is not interpreted by the Element Manager. The table cell contents can be copied into a third party application for interpretation.
- **Length**— Length of the payload, byte counter, decimal display format. Since the payload can be longer that the maximum 32 bytes retained by the log, this value displays how many bytes are actually in the frame.
- **Payload**—The payload portion of the data box.
- **SOF**—The string that contains the Start of Frame code abbreviation. Place the cursor over a cell in this column to display descriptions of the abbreviation.
- **EOF**—The string that contains the End of Frame code abbreviation. Place the cursor over a cell in this column to display descriptions of the abbreviation.

## Change button

If Administrator or Maintenance user rights are set to access the button. you can display the Embedded Port Log Settings Dialog box. If you do not have access to this button, an error dialog box appears.

This dialog box log provides a detailed history log of all traffic passing through the embedded port, as shown in Figure 60.

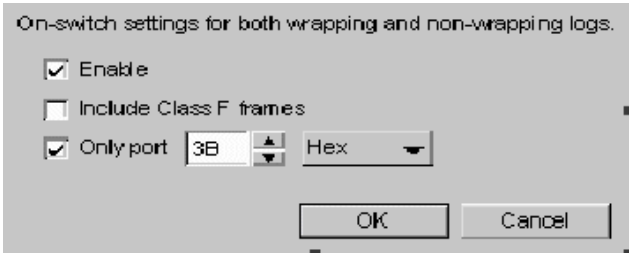



**Figure 60** Log Settings dialog box

**NOTE:** If not in FICON style mode, the Hex/Dialog option is not displayed and entries are only made in decimal.

- **Enable**—Turns logging on (default=checked) or off (unchecked) for the currently displayed log (either wrapping or. Implemented on the switch as trace filter set to no ports (TRACE_NO_PORTS).
- **Include Class F Frame**—When this option is checked, which is the default, all frames received are stored in the log, unless port filtering logs only one port. When unchecked, no Class F frames are logged.

- **Only Port**—When this option is unchecked, which is the default, frames from all ports are logged. F frames depend on the **Include Class F Frame** option. When checked, the port entry box is enabled, and the port number to be logged can be entered. When in FICON Style mode-, port numbers can be entered into this box in either in hex or decimal using **Hex/Decimal**. The spin button limits port number entries to valid ranges, including the exclusion of unavailable port numbers. After selecting **OK** from this port selection dialog, the selected port number is displayed on the main log dialog next to the **Only port** check box (such as, **Only port 59**, or **Only port 59 (3B)** if in FICON style mode). Only frames from or to the selected port are retained in the switch's log after that point.

# Switch Fabric log (Advanced log)

The Switch Fabric log includes switch fabric information as shown in Figure 61.

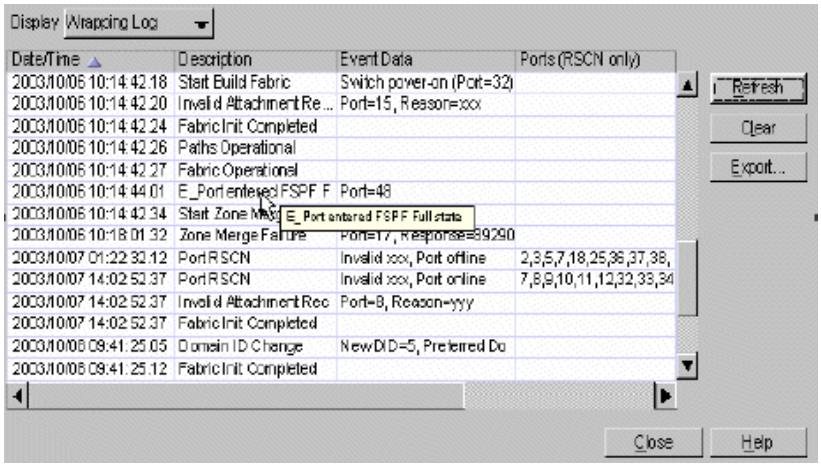



**Figure 61** Switch Fabric log

This log displays the following information about switches in a fabric:

- **Non-wrapping Log or Wrapping Log**—From the submenu, select **Non-wrapping log** or **Wrapping log**. **Wrapping log** is the default.
- **Date and Time**—The date and time that the event occurred. The format is *yyyy/mm/dd hh:mm:ss:tt*. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Description**—The description string for the event type. The string content is displayed directly as stored in the log.
- **Event Data**—This string contains details of the event, and is variable depending on the event logged. This is provided directly by the log content, and is displayed here exactly as received.
- **Ports (RSCN only)**—For Port RSCN events only, a list of affected ports is displayed in this column. This is interpreted from port bitmap data stored in the log, and only the ports with a bit value of 1 are listed. If there are many bits set in a large switch, the contents of this box can be very long.

# 5 Using maintenance features

This chapter describes how to use the options that display from the Maintenance menu on the Element Manager menu bar. The chapter includes the following topics:

# Running port diagnostics

The **Port Diagnostics** option enables you to run internal and external loopback tests on any port or all ports on a port card. At the start of the loopback test, the port or port card can be online, offline, blocked, or unblocked

- **Internal loopback test** —An internal loopback test checks port circuitry, but does not check fiber-optic components of a port transceiver. The test is performed with a device attached to the port, but the test momentarily blocks the port and is disruptive to the attached device.

  An optical transceiver (SFP or XFP) must be installed in the port during the test. A device can remain connected during the test.
- **External loopback test** —An external loopback test checks port circuitry, including fiber-optic components of a port transceiver. To perform the test, the attached device must be acquiesced and disconnected from the port, and a multimode or singlemode loopback plug must be inserted in the port receptacle.

To use this option, follow the detailed steps in the appropriate service manual for your Edge Switch.

# Swapping ports (FICON Management Style)

**NOTE:** This procedure applies only to the Edge Switch 2/32. FICON Management Style is not available on the Edge Switch 2/24.

Select **Swap Ports** to display the Swap Ports dialog box. Use this dialog box to swap one port address for another. For example, if the current address for port 0 is 04 and the current address for port 1 is 05, you can swap so that the address for port 0 is 05, and the address for port 1 is 04.

**NOTE:** Before swapping ports, make sure that the system administrator varies devices offline that are attached to the ports whose addresses you are going to swap. Ports to be swapped are blocked during this procedure, because swapping ports is disruptive to port operation.

To swap ports, use the following steps:

1. Select **Maintenance > Swap Ports**. The Swap Ports dialog box appears, as shown in Figure 62.

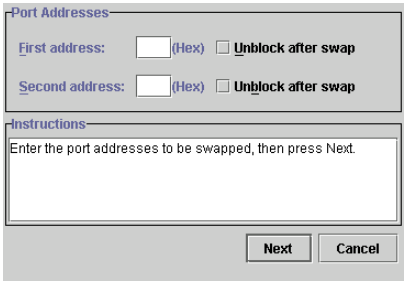



**Figure 62** Swap Ports dialog box

2. Enter the first address (in hexadecimal format).
3. If you want to unblock the port, click **Unblock after swap**. Note that ports are automatically blocked during the swap process.
4. Enter the second address (in hexadecimal format).
5. If you want to unblock the port, click **Unblock after swap**.
6. Click **Next** to continue.
7. Follow the on-screen instructions and click **Next** to continue through to the next screen.
8. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

# Collecting maintenance data

The Data Collection option enables you to collect maintenance data that can help support personnel diagnose system problems. Save this data to a zip file on a CD (or other medium with the appropriate capacity), and forward it to technical support personnel.

**NOTE:** If the Full Volatility feature has been enabled through the switch's maintenance port, a memory dump file will not be included with the data collection.

To use this option, follow the detailed steps in the appropriate service manual for your Edge Switch.

# Executing an IPL

**CAUTION:** The Ethernet connection between the HAFM appliance and switch is interrupted momentarily during an initial program load (IPL). However, this does not interrupt Fibre Channel traffic.

△ **CAUTION:** An IPL is not intended for ordinary or casual use and should only be performed if the control processor (CTP) is suspected to be faulty. Do not use this option unless directed by your support representative or if you need to set the CTP.

If it is necessary to execute an IPL on the switch, use the following steps:

1. Select **Maintenance > IPL**. A dialog box appears prompting you to continue the IPL.

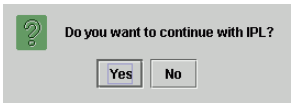



**Figure 63** IPL Confirmation dialog box

2. If you want to continue the IPL, click **Yes**.

Selecting **IPL** causes the Ethernet connection between the switch and HAFM appliance to drop momentarily. It also causes the following to occur in the Element Manager window:

- As the network connection drops, the switch **Status** table on the Hardware View turns yellow.
- The **Status** box in the table displays `No Link` and the **State** box displays the reason for no link.
- A gray square appears in the status bar. See Table 2 on page 37 for an explanation of this status bar display.
- The FRUs illustrated in the Hardware View do not display. They display again after the connection is re-established.

An IPL initiates the following functions in the switch:

- Restarts the operational firmware on the CTP card and executes abbreviated power on system tests (POSTs). Then, if no POST errors are encountered, the switch resumes the active role that it had before the IPL.
- Resets the Ethernet interface on the CTP card, causing the connection to the HAFM appliance to drop momentarily. The status icon for the switch in the Physical/Topology Map will change to a gray square until the connection is reestablished.

After the IPL:

- All Fabric services databases containing information about current Fabric logins, name server registrations, and other data remain intact, making the operation transparent to attached devices.
- The switch returns to the online state, even if it was offline before the operation.
- All ports configured as blocked will remain blocked.

# Setting online state

Use the procedure in this section to display the current switch operating state (offline or online) and change the state as required. See Table 2 on page 37 for more information on the switch operating states.

△ **CAUTION:** Before setting the switch offline, warn administrators and users currently operating devices that are attached to the switch that it is going offline and that there will be a disruption of communications. Make sure administrators of devices attached to ports halt Fibre Channel traffic through the switch.

To set the switch online or offline (depending on current state):

1. Right-click the switch in the Hardware View and select **Set Online State**, or click **Maintenance > Set Online State**. One of the following dialog boxes appears, depending on the current operating state.

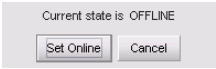



**Figure 64** Set Online State dialog box (state is offline)

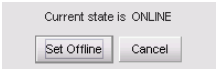



**Figure 65** Set Online State dialog box (state is online)

2. Click **Set Offline** or **Set Online**, depending on the operating state you want to set.
3. When a warning box appears requesting you to confirm the offline or online state, click **OK**.

As the switch goes offline, `OFFLINE` appears in the **State** box of the **Switch Status** table in the Hardware View.

# Managing firmware versions

Firmware refers to the internal operating code for the switch. You can maintain up to eight firmware versions on the HAFM appliance for downloading to an switch. To use the **Firmware Library** option to manage firmware versions, follow the steps in the appropriate service manual for your Edge Switch.

# Enabling e-mail notification

E-mail addresses and the SMTP server address for e-mail notification of switch events must be configured through HAFM. Refer to the *HP StorageWorks HA-Fabric Manager user guide* for instructions on configuring e-mail notification.

**NOTE:** E-mail recipients are configured in HAFM through the E-Mail Event Notification Setup dialog box. A valid SMTP address is configured through this dialog box.

Use the Enable E-Mail Notification function on the Element Manager to enable e-mail notification for events that occur on a selected switch. The default state is disabled.

To enable and disable e-mail notification, select **Maintenance > Enable E-Mail Notification**. Click this option again to disable it.

# Enabling or disabling call home notification

Select **Maintenance > Enable Call Home Notification** to enable and disable Call Home Notification for system problems. A check mark appears next to this option when the Call Home Notification is enabled.

# Backing up and restoring configuration

Select **Maintenance > Backup & Restore Configuration** to save the product configuration stored on the switch to the HAFM appliance hard disk or to restore the product configuration from the HAFM appliance. Only a single copy of the configuration is kept on the HAFM appliance.

Backup is primarily for single-CTP systems, such as the Edge Switch 2/24, where a backup is needed to restore to a replacement CTP card. You can also use this feature for a special purpose configuration or for temporary testing of a configuration. You cannot modify the location and file name of the saved configuration.

**NOTE:** You can only restore the configuration to a switch with the same IP address.

**NOTE:** For the optional SANtegrity Binding feature, Backup and Restore Configuration will backup and restore Switch Binding information, but will not back up and restore Fabric Binding and Enterprise Fabric Mode information.

## Backup procedure

Use the following procedure to back up your product configuration:

1. Select **Maintenance > Backup & Restore Configuration** to display the Backup and Restore Configuration dialog box.

   The Backup and Restore dialog box includes a short description of the features performed when you click **Backup** or **Restore**.

   Following is a list of configurations that are backed up to the HAFM appliance:

   - Identification data (switch name, description, and location).
   - Port configuration data (port names, blocked states, and extended distance settings).
   - Operating parameters for fabric (E_D_TOV, R_A_TOV, switch priority, interop mode) and for switch (preferred domain ID, rerouting delay, and domain RSCNs).
   - SNMP configuration (trap recipients, community names, and write authorizations).
   - Zoning configuration (active zone set and default zone state).
   - Alternate Control Prohibited Settings.
2. To back up data, click **Backup**.

3. When the dialog box appears confirming that the backup is complete, click **OK**. If the backup fails, a dialog box appears to inform you that the backup to the HAFM appliance failed.

## Restore Procedure

Use the following procedure to restore your product configuration:

1. Set the switch offline before performing the restore function.
2. Click **Restore** on the **Backup and Restore Configuration** dialog box to restore the backed up configuration to the nonvolatile random access memory (NV-RAM) on the switch. Note that the restore operation initiates an IPL. See "Executing an IPL" on page 135 for more information about IPLs.

**NOTE:** Set the switch to offline before performing the restore function. If you click **Restore** and the switch is online, a message dialog appears requesting that you turn the switch offline. No action takes place when you close the dialog box. For instructions on setting the switch offline or online, see "Setting online state" on page 136.

If the switch is already offline and you click **Restore**, a confirmation dialog box appears indicating that the restore will overwrite any existing configuration already on the switch. The dialog box also displays the date of the restored backup. Click **OK**.

# Resetting configuration

**NOTE:** You must have maintenance authorization feature permissions to access this feature.

This option resets all configuration data input through options in the **Configuration** menu, zoning configurations, and switch addressing to factory-default values. Since the current IP address for the switch may not match the factory default address, the Ethernet link between the switch and the HAFM appliance may drop and not reset.

Before using this option, record the switch's current IP address, which appears below the switch's icon in the HAFM Physical/Topology Map view (**Display Options** set to **Network Address**). You can also find the current IP address through the EWS interface.

After resetting the configuration, you must reset the original address on the switch through the maintenance port or the EWS interface to maintain LAN connections and communication with the HAFM appliance.

Use the following procedure to reset your product configuration:

1. Set the switch offline. For instructions, see "Setting online state" on page 136.
2. Select **Maintenance > Reset Configuration**. The following warning displays:

```
CAUTION! This operation will reset all switch configuration data and
non-volatile settings to factory default values. All optional features will
also be disabled. The switch must be offline to continue.
```

**NOTE:** If you have enabled features that add additional port function since the switch was shipped from the factory, these features will be disabled (factory default) when the configuration is reset. Only those ports that were enabled at the factory will function. You will have to enable the additional port function features again through the Configure Feature Key dialog box. See "Configuring a feature key" on page 104 for more information.

**NOTE:** If you have enabled the Full Volatility feature through the switch's maintenance port since the switch was shipped from the factory, this feature will be disabled (factory default) when the configuration is reset.

**NOTE:** Factory default values may vary, depending on the firmware release installed in your switch. For a list of values, refer to the appropriate service manual for your Edge Switch.

3. Click **Reset** to reset all configuration data.

**NOTE:** If you have changed the switch's IP addressing from the factory default value, you may not recover the Ethernet connection between the switch and the HAFM appliance because the Internet Protocol (IP) address will reset to the factory default during this procedure.

For complete steps in recovering this connection, refer to the Reset Configuration Data procedure for the Element Manager in the appropriate service manual for your Edge Switch.

# 6 Optional features

This chapter provides detailed information on using, administering, and configuring optional HAFM application features through the Element Manager. There are two types of features covered in this chapter:

- Keyed features, requiring feature keys to be purchased and enabled through the Configure Feature Key dialog box in the product's Element Manager.
- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through the HAFM or Element Manager.

This chapter includes the following topics:

# Preferred Path

The Preferred Path feature enables you to influence the route of data traffic when traversing more than one Switch in a fabric. If more than one ISL connects switches in your SAN, this feature will be useful for specifying an ISL preference for a particular flow. The data path consists of the source port of the Switch or Director being configured, the exit port of that Switch or Director, and the domain ID of the destination Switch or Director. Each Switch or Director must be configured for its part of the desired path in order to achieve optimal performance. You may need to configure Preferred Paths for all Switches or Directors along the desired path for proper multi-hop Preferred Path operation.

## Configuring a Preferred Path

The Preferred Path feature enables you to influence the route of data traffic when traversing multiple switches or directors in a fabric. If more than one ISL connects switches in your SAN, this feature will be useful for specifying an ISL preference for a particular flow. The data path consists of the following:

- Source port of the switch or director being configured
- Exit port of that switch or director
- Domain ID of the destination switch or director.

Each switch or director must be configured for its part of the desired path in order to achieve optimal performance. You may need to configure Preferred Paths for all switches or directors along the desired path for proper multi-hop Preferred Path operation. The following is an example of the procedure to use.

## Adding a preferred path

To add a new preferred path, use the following steps:

---

△ **CAUTION:** Activation of a new Preferred Path will cause a reroute to occur if the Preferred Path is different from the current path. In congested environments, with traffic on the current path, a reroute can cause an out of order frame (OOOF) at the destination device.

- Reroutes are a natural activity in any Fibre Channel fabric when the network is modified. For example, reroutes occur when ISLs are added or lost or when new switches are added to the fabric. Fibre Channel devices are designed to handle errors like OOOFs, but some send error messages when they occur.
- In FICON environments, an IFCC error can result from an OOOF. To avoid these error messages, devices should be varied offline before a Preferred Path is activated, and returned to online status after the activation.

---

1. Select **Configure > Preferred Path**. The Configure Preferred Paths dialog box appears as shown in Figure 66. The Configure Preferred Paths dialog box provides the configuration for a single switch's preferred path.

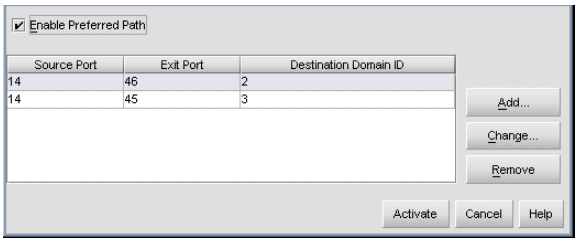



**Figure 66** Configure Preferred Paths dialog box

**NOTE:** Some columns may only display when the FICON Management Style feature has been installed.

**The columns included in the dialog box are as follows:**

- **Source Port**—This column lists the source port of the preferred path.
- **Source Addr** (FICON management style only)—This column lists the source address of the preferred path.
- **Exit Port**—This column lists the exit port of the preferred path.
- **Exit Addr** (FICON management style only)—This column lists the exit address of the preferred path.
- **Destination Domain ID**—This column lists the domain ID of the destination switch or director. The range of the destination domain ID number is 1 through 31.

**TIP:** You may need to configure preferred paths on multiple switches or directors to optimize load balancing for an entire path between devices.

**NOTE:** A warning message will display if the switch or director has not been configured for insistent domain ID. If this is the case, close the dialog box and select **Configure > Operating Parameters > Switch Parameters**. Select the **Insistent** check box in the Configure Switch Parameters dialog box. Return to the Configure Preferred Paths dialog box and continue to step 2.

2. Click **Add** to configure a new preferred path. The Add Preferred Path dialog box appears as shown in Figure 67.

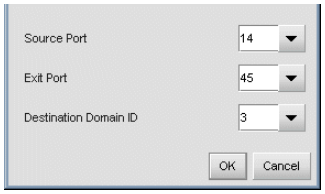



**Figure 67** Add Preferred Path dialog box

3. Click the drop-down lists for the **Source Port**, **Exit Port**, and **Destination Domain ID** to make your choices. See "Exporting the Configuration Report" on page 115 for more information.

**TIP:** You can also enter an exit port number for future or offline environments.

4. Click **OK**. The new route will be added to the table on the Configure Preferred Paths dialog box. The configuration will be validated.
5. Select the **Enable Preferred Paths** check box in the Configure Preferred Paths dialog box to enable the configured preferred paths. When this option is not selected, the preferred path configurations are not enforced, but the configured paths are retained for future use.
6. Click **Activate**.

## Changing a preferred path

To change a preferred path, use the following steps:

1. Select **Configure > Preferred Path**. The Configure Preferred Paths dialog box appears as shown in Figure 66.
2. To change a preferred path, select the path you want to change and click **Change**. The Change Preferred Path dialog box appears.
3. Change the data as required.
4. Click **Activate**. The data will be changed in the table on the Configure Preferred Paths dialog box.
5. Click the **Enable Preferred Paths** check box in the Configure Preferred Path to enable the configured preferred paths. When this option is not selected, the preferred path configurations are not enforced, but the configured paths are retained for future use.
6. Click **Activate**.

## Removing a preferred path

To remove a new preferred path, use the following steps:

1. Select **Configure > Preferred Path**. The Configure Preferred Paths dialog box appears as shown in Figure 66.
2. Select the path you want to remove and click **Remove**.
3. Click **Activate**.

## Specifying preferred path example

Figure 68 shows a portion of a more complex SAN. In this example, we will do the following:

- Specify a path between the Source Device and Destination Device A, going through Switch1, Switch 2, and Switch 3 (the desired data flow is shown as Data Flow 1).
- Enter data through port 14
- Exit data through port 45
- Make Switch 3 the destination device

Use the following procedure to accomplish the above tasks.

1. Select **Configure > Preferred Path** in Switch 1's Element Manager window to configure the path on Switch 1. The Add Preferred Path dialog box appears.
2. Click **14** in the **Source Port** field.
3. Click **45** in the **Exit Port** field.
4. Click **3** (Switch 3's domain ID) in the **Destination Domain ID** field.

This procedure only specifies that data will enter and exit Switch 1 through specific ports on its way to Switch 3. This process does not specify a Preferred Path for data moving through Switch 2. To specify paths through Switch 2 (Figure 69 on page 148), we will do the following:

- Enter data through port 11
- Exit data through port 21
- Make Switch 3 the destination device

Use the following procedure to accomplish the above tasks:

1. Select **Configure > Preferred Path** in Switch 2's Element Manager window to configure the path on Switch 2. The Add Preferred Path dialog box appears.
2. Click**11** in the **Source Port** field.
3. Click **21** in the **Exit Port** field.
4. Enter **3** (Switch 3's domain ID) in the **Destination Domain ID** field.

The primary choice for data movement will be from the Source Device in port 14 and out port 45 on Switch 1, in port 11 and out port 21 on Switch 2, and through Switch 3 to either Destination Device A or B.

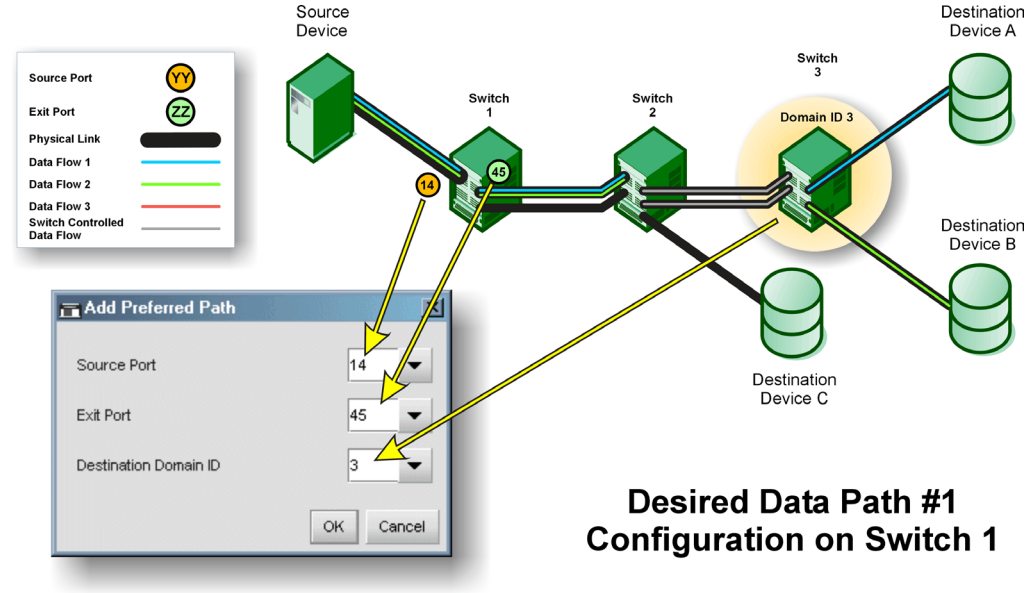



**Figure 68** Specifying preferred path for switch 1

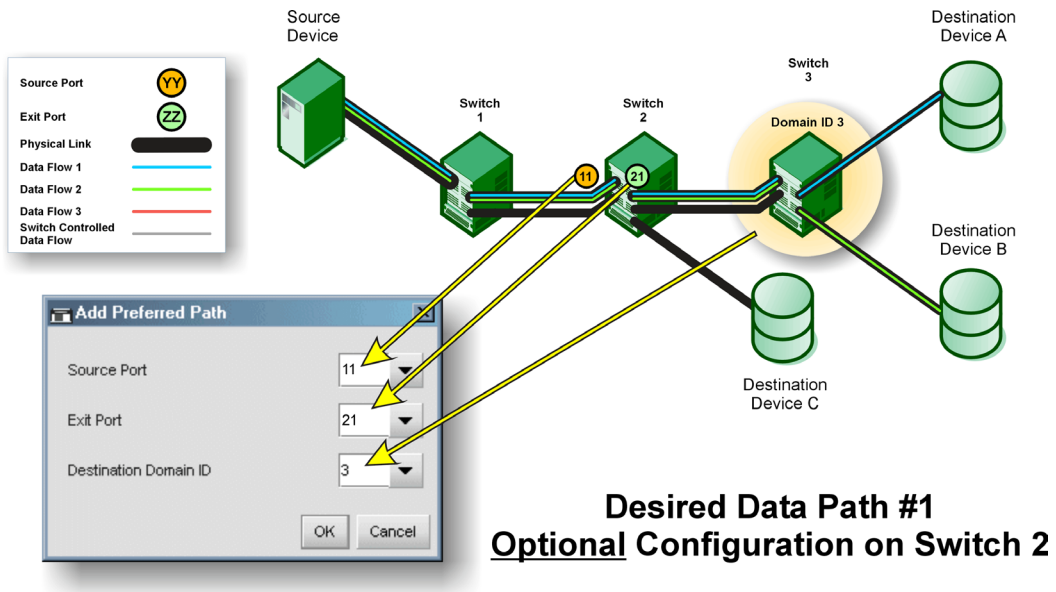



**Figure 69** Specifying preferred path for switch 2

The following rules apply when configuring preferred paths:

- The switch's domain ID must be set to **insistent**.
- Domain IDs must be in the range of 1 through 31.
- The specified numbers for Source Ports and Exit Ports must be in the range equal to the number of ports for the switch being configured.
- For any source port, only one path may be defined to each destination domain ID.

To install and enable this option, select the **Features** option under the Element Manager's **Configure** menu. See "Configuring a feature key" on page 104.

# FICON Management Server

**NOTE:** The FICON Management Server feature is available only for the Edge Switch 2/32. The FICON Management Server feature is not available on the Edge Switch 2/24.

The FICON Management Server is a keyed feature that allows host control and inband management of the switch through an IBM System/390 or zSeries 900 Parallel Enterprise Server server attached to a switch port. The server communicates with the switch through a FICON channel. Control of connectivity and statistical product monitoring are provided through a host-attached console.

## Installing the FICON Management Server

To install and enable the FICON Management Server, select **Configure > Configure Feature Key**. For more information, see "Configuring a feature key" on page 104.

## Configuring the FICON Management Server

To configure the FICON Management Server, use the following steps:

1. Select **Configure > FICON Management Server**.
2. Select the **Enable FICON** check box to enable the Management Server. (To disable the Management Server, click the check box again to remove the check mark.)
3. Click **Parameters** to open the Configure FICON Management Server Parameters dialog box. (See "FICON Management Server parameters" on page 150 for details about the parameters you can set.)
4. Enable or disable switch clock alert mode by clicking **Switch Clock Alert Mode**. When a check mark appears, the alert mode is enabled.
5. Allow or prohibit host control by clicking **Host Control Prohibited**. When a check mark appears, host control is prohibited.
6. Allow or prohibit offline state control by clicking **Programmed offline state control**. When a check mark appears, programmed control of the offline state is allowed.
7. If necessary, click a code page from the **Code Page** drop-down list.
8. Activate changes and close the dialog box by clicking **Activate**.

9. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration data" on page 117.

## FICON Management Server parameters

The following provides a detailed description of the parameters you can set when you configure the FICON Management Server:

- **Switch Clock Alert Mode**—Click this check box to display a check mark and enable Clock Alert Mode. If this is enabled, the following occurs when users set the date and time through the Configure Date and Time dialog box (**Configure** menu):
  - If you enable **Periodic Date/Time Synchronization**, an error message appears, indicating that clock alert mode must be cleared to enable automatic synchronization of the date and time.
  - If you manually set the date and time (**Periodic Date/Time Synchronization** is not enabled), a confirmation dialog box will display. You must click **OK** on that dialog box to continue manual configuration.
- **Host Control Prohibited**—Click this check box to display a check mark and prohibit a host management program from changing configuration and connectivity parameters on the switch. In this case, the host program will only have read authorization and cannot make changes. When the check mark is not displayed, a host program can change configuration and connectivity parameters on the switch.
- **Programmed offline state control**—Click this check box to display a check mark and enable a host management program to control the switch's offline and online state. When a check mark is not displayed, a host program cannot set the switch online or offline.
- **Code Page**—Use this option to set the language required for the port name that appears on the Management Server. Language support is provided through character set 697 for all Extended Binary-Coded Decimal Interchange Code (EBCDIC) pages.

  When planning the installation, choose the EBCDIC code page for displaying host-assigned port names or the CUP name. As an example, if the code page for Italy is selected and a port name is assigned in Italian by the host management program, the Italian language port name appears in the Element Manager.

  The drop-down list displays the code pages that are available for configuration. The default code page is United States/Canada 00037. Refer to Table 6 for other code pages.

**Table 6** Available code pages

| Code page name | Code page | Hexadecimal CPGID |
|---|---|---|
| United States/Canada | 00037 | 0025 |
| Germany/Austria | 00273 | 0111 |
| Brazil | 00275 | 0113 |
| Italy | 00280 | 0118 |
| Japan | 00281 | 0119 |
| Spain/Latin America | 00284 | 011C |

**Table 6** Available code pages (continued)

| Code page name | Code page | Hexadecimal CPGID |
|---|---|---|
| United Kingdom | 00285 | 011D |
| France | 00297 | 0129 |
| International #5 | 00500 | 01F4 |

# Open Systems Management Server

**NOTE:** Open Systems Management Server (OSMS) is available only for the Edge Switch 2/32. OSMS is not available on the Edge Switch 2/24.

The Open System Management Server (OSMS) is a feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device. This device is attached to a director or switch port. The device communicates with the switch or director through Fibre Channel common transport (FC-CT) protocol.

## Configuring the Open Systems Management Server

Use these procedures to configure the Open Systems Inband Management program to function with the switch.

To configure the Open Systems Management Server, use the following steps:

1. Select **Configure > Management Server**.
   Two submenu options display, as shown in step 2 and step 3:
2. Click **Enable the Open System Management Server**. (To disable the open systems management server, click the check box again to remove the check mark.)
3. Click **Host Control Prohibited** to display a check mark and prohibit the host management program from changing configuration and connectivity parameters on the switch. In this case, the host program has read-only access to configuration and connectivity parameters. Clicking the check box when it contains a check mark removes the check mark and allows a host program to change configuration and connectivity parameters on the switch.
4. Click **Activate** to implement changes and close the dialog box.
5. If you are finished configuring the switch, back up the configuration data. For more information, see "Backing up and restoring configuration" on page 138.

# SANtegrity features

SANtegrity includes a set of features that enhance security in SANs (Storage Area Networks) that contain a large and mixed group of fabrics and attached devices. Through these features, you can allow or prohibit switch attachment to fabrics and device attachment to switches. These features are enabled by purchasing a feature key, then enabling the key through the Configure Feature Key

dialog box. For general instructions in enabling a feature key, see "Configuring a feature key" on page 104.

SANtegrity binding features include:

- Fabric binding
- Switch binding

**Enterprise Fabric Mode** - Although this is not a keyed feature the SANtegrity Fabric Binding and Switch Binding must be installed before you can use the Enterprise Fabric Mode function through the HAFM **Fabrics** menu.

## Fabric binding

This feature is managed through the Fabric Binding option, available through the **Fabrics** menu in HAFM when the **Fabrics** tab is selected. Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

### Enable/disable and Online State functions

For Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the switch is offline or online.

Be aware of the following:

- Because switches are bound to a fabric by World Wide Name (WWN) and domain ID, the **Insistent Domain ID** option in the Configure Switch Parameters dialog box is automatically enabled if Fabric Binding is enabled.
- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director or switch is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

For more information about how to enable, disable, and configure this option, refer to the Fabric Binding section of the *HP StorageWorks HA-Fabric Manager user guide*.

# Switch binding

This feature is managed through the Switch Binding submenu options available on the Element Manager Configure menu. Using Switch Binding, you can specify WWNs for devices and switches that can attach to director and switch ports. When an unauthorized WWN attempts to log in, an event is posted to the Event Log. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a switch or director.

## Configuring switch binding overview

To configure Switch Binding, you must first activate the feature using the Switch Binding State Change dialog box while choosing the type of port where you want to restrict connection (connection policy). Possible choices are E_Ports, F_Ports, or all types.

If the switch is online, activating Switch Binding populates the Membership List in the Switch Binding - Membership List dialog box (Element Manager) with the following WWNs currently connected to the switch, depending on the connection policy set in the State Change dialog box:

- WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.
- WWNs of switches connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached switch.
- WWNs of devices connected to F_Ports and switches connected to E_Ports (all-ports connection policy).

### Notes:

- When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, switches, or both that are currently connected to the switch.
- If the switch is offline and you activate Switch Binding, the Membership List is not automatically populated.
- Edits to the Switch Binding Membership List will be maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and/or switches from connecting with switch ports by removing them from the Membership List in the Switch Binding Membership List dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and switches as well.

## Enabling or disabling switch binding

Use the following procedure to enable or disable Switch Binding:

1. Select **Configure > Switch Binding > Change State**. The Switch Binding State Change dialog box appears.


**Figure 70** Switch Binding State Change dialog box

2. Perform one of the following steps:
   - To disable Switch Binding, click **Enable Switch Binding** to clear the **Enable Switch Binding** check box, then click **Activate**.
   - To enable Switch Binding, click **Enable Switch Binding** to add a check mark. Then, go to step 3 to set the Connection Policy.
3. Click one of the **Connection Policy** option buttons.
   - **Restrict E_Ports**—Restricts connections from specific switches to switch E_Ports. Switch WWNs can be added to the Switch Membership List to allow connection and can be removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.
   - **Restrict F_Ports**—Restricts connections from specific devices to switch F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and can be removed from the Membership List to prohibit connection. Switches are allowed to connect to any E_Port.
   - **Restrict All**—Restricts connections from specific devices to switch F_Ports and switches to switch E_Ports. Device and switch WWNs can be added to the Switch Membership List to allow connection and can be removed from the Membership List to prohibit connection.
4. Click **Activate** to enable the changes and close the dialog box.
5. Edit the Switch Membership List through the Switch Binding Membership List dialog box to add or remove switches and devices that are allowed to connect with the switch. See "Editing the Switch Membership list" on page 155 for procedures.

## Editing the Switch Membership list

Use the following procedure to edit the switch membership list:

1. Select **Configure > Switch Binding > Edit Membership List**. The Switch Binding Membership List dialog box appears. The WWNs of devices and/or switches that can currently connect to switch ports are listed in the **Switch Membership List** panel.

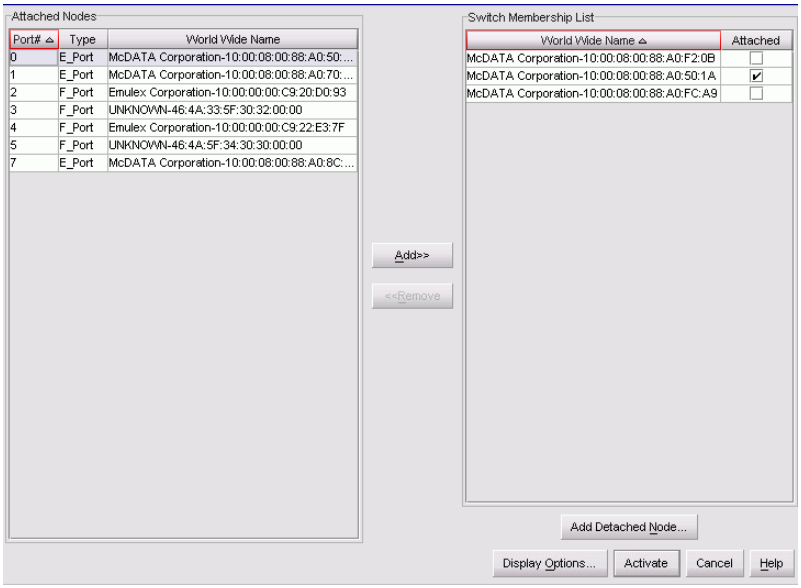



**Figure 71** Switch Binding Membership List dialog box

**NOTE:** See "Configuring switch binding overview" on page 153 for information on how the Switch Membership List is populated with WWNs according to options set in the Switch Binding State Change dialog box.

2. If nicknames are configured for WWNs through HAFM and you want these to display instead of WWNs in this dialog box, click the **Display Options** button at the bottom of the dialog box. When the Display Options dialog box appears, click **Nickname**, then **OK**.
3. To prohibit connection to a switch port from a WWN currently in the Membership List, click the WWN or nickname in the Membership List, then click the **Remove** button. The WWN or nickname will move to the **Attached Nodes** panel. WWNs can only be removed from the fabric if any of the following is true:
   - The switch is offline.
   - Switch Binding is disabled.
   - The switch or device with the WWN is not connected to the switch.

- Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to Restrict F_Ports.
- The switch or device with the WWN is connected to a port that is blocked.
- The switch or device with the WWN is not currently connected to the switch (detached node).

4. You can add WWNs to the **Switch Membership List** (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a switch port from a WWN in the **Attached Node** panel, click the WWN or nickname in the **Attached Node** panel, and then click **Add**. The WWN or nickname will move to the **Membership List** panel.
5. To add a WWN for a device or switch not currently connected to the switch, click the **Detached Node** button. When the Add Detached Node dialog box appears, enter the appropriate WWN or nickname (if configured through HAFM) and click **OK**. The WWN or nickname appears in the **Switch Membership List**.
6. Click **Activate** to enable the changes and close the dialog box.

## Enable/Disable and Online State functions

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online.

Be aware of the following:

- Switch Binding can be enabled or disabled whether the switch is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.
- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.
- WWNs can only be removed from the Switch Membership List if any of the following are true:
  - The switch is offline.
  - Switch Binding is disabled.
  - The switch or device with the WWN is not connected to the switch.
  - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to Restrict F_Ports.
  - The switch or device with the WWN is connected to a port that is blocked.
- If the switch is online and Switch Binding is not enabled, all nodes and switches attached to the switch are automatically added to the Switch Membership List.

## Zoning with Switch Binding enabled

Note that SANtegrity Binding has no effect on existing zoning configurations. However, note that if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the device cannot log in to the director or switch port and cannot connect to other devices in the zone with Switch Binding enabled.

# Enterprise Fabric Mode

**Enterprise Fabric Mode** is an option available on the **Fabrics** menu of HAFM if the SANtegrity Binding feature key is installed. This option automatically enables the following features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. Note that there are specific requirements for disabling these parameters and features when the director or switch is offline or online.

## Features and parameters enabled

The following features and parameters are enabled by the **Enterprise Fabric Mode** option:

- Fabric binding

  This is a SANtegrity Binding feature enabled through the **Fabrics** menu in HAFM that allows or prohibits switches and directors from merging with a selected fabric. See "Enable/disable and Online State functions" on page 152 for details on enabling/disabling Fabric Binding with Enterprise Fabric Mode enabled.

- Switch binding

  This is a SANtegrity Binding feature enabled through the **Configure** menu in the Element Manager that allows or prohibits switches and/or directors from connecting to switch E_Ports, and prohibits devices from connecting to F_Ports. See "Enabling or disabling switch binding" on page 154 for details on enabling/disabling Switch Binding with Enterprise Fabric Mode enabled.

- Rerouting delay

  This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the Element Manager.

  Rerouting Delay ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order because frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

  If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** box of the Configure Fabric Parameters dialog box (Configure menu). This delay enables frames sent on the old path to exit to their destination before new frames begin traversing the new path.

  If Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless the switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode.

- Domain RSCNs

  This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the Element Manager. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to HBAs and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

  If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode.

- Insistent Domain Identification (ID)

  This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the Element Manager. Enabling this option sets the domain ID configured in the **Preferred Domain ID** box in the Configure Switch Parameters dialog box as the active domain identification when the fabric initializes. A static and unique domain identification is required by the Fabric Binding feature because the feature's Fabric Membership list identifies switches by WWN and Domain ID. If a duplicate preferred domain ID is used, then insisted, warnings occur when directors and switches are added to a Fabric Membership List.

  If Fabric Binding or Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless these options are disabled or the switch is offline. Disabling insistent domain ID will disable Enterprise Fabric Mode and Fabric Binding.

## For More Information

See "Enable/disable and Online State functions" on page 152 for Fabric Binding and "Enabling or disabling switch binding" on page 154 for Switch Binding.

To enable and disable this option, refer to the Enterprise Fabric Mode section of the *HP StorageWorks HA-Fabric Manager user guide*.

# Open Trunking

Interswitch links (ISLs) connect ports between E_Ports on Fibre Channel switches and link these switches into a multiswitch fabric. Multiple ISLs may be connected between the switches in the fabric. Data from an attached end device (server or storage) flows through these ISLs to a target end-device connected to a switch somewhere in the fabric. A data flow is data received from a specified receive port that is destined for a port in a specified target domain (switch). The list of ISLs that are candidates for being rerouted (to or from) is derived from the fibre shortest path first (FSPF) algorithm.

The Open Trunking feature monitors the average data rates of all traffic flows on ISLs (from a receive port to a target domain), and periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and to optimize bandwidth use. The objective of open trunking is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

Load balancing among the ISLs does not require user configuration, other than enabling Open Trunking. However, you can modify default settings for congestion thresholds (per port) and the Low BB_Credit Threshold if desired.

In particular, you do not need to manually configure ISLs into *trunk groups* of redundant links where data can be *off-loaded*. Candidate links for rerouting flow are identified and maintained automatically. This means that flow may be rerouted onto a link that goes to a different adjacent switch, as long as that link is on the least cost/shortest path to the destination domain ID.

To install and enable this option, select **Configure > Configure Feature Key**. See "Configuring a feature key" on page 104.

## Enabling and configuring Open Trunking

To enable Open Trunking for a specific switch and configure threshold values and event notification options, use the following steps.

1. Select **Configure > Open Trunking**.
   The Configure Open Trunking dialog box appears.

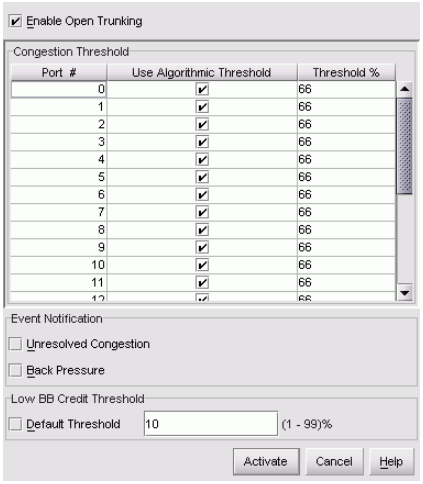



**Figure 72** Configure Open Trunking dialog box

2. Click **Enable Open Trunking** to display a check mark and enable Open Trunking.
3. Set the **Congestion Thresholds** for ports as percentages of link bandwidths, in the range of 1% through 99%. These thresholds are used only when a port becomes an ISL. When the link's traffic load becomes greater than this percentage, the link is seen as *congested* and traffic is rerouted (if possible) to an uncongested link. Note that rerouting may not be possible if there are no alternate links available, or if alternate links are congested or lack BB_Credits.

**NOTE:** Using default settings for port congestion thresholds should work well in most cases. Normally, you will not need to set them.

Set the **Congestion Threshold** using one of these methods:

- Click the check box under the **Use Algorithmic Threshold** column to display a value under the **Threshold %** column. This value is computed by the feature's rerouting algorithm. If you click this check box, you cannot enter a value into the **Threshold %** column for the port.

**NOTE:** If you clear the check box, any value that was set in the **Threshold %** column for the port redisplays.

- Click in the **Threshold %** column and enter a value in the range of 1 through 99.

**NOTE:** You must either specify a value in the **Threshold %** column or click the **Use Algorithmic Threshold** check box.

4. Set **Event Notification** options. Note that, if enabled, these notifications occur the first time the events occur. Notifications are not resent while the problem persists.
   - **Unresolved Congestion**. Click this check box to enable notification. If enabled, an *unresolved congestion* entry is made to the Event Log and an SNMP trap is generated if trap recipients are configured through the Configure SNMP dialog box.

**NOTE:** An unresolved congestion event occurs when the rerouting algorithm cannot find a path for rerouting data flow and relieving congestion on an ISL.

   - **Back Pressure**. Click this check box to enable this option. If enabled, a back pressure entry will be made to the Event Log and an SNMP trap will be generated if trap recipients are configured through the Configure SNMP dialog box.

     A back pressure event occurs when the percentage of time the ISL lacks BB_Credits exceeds the threshold. A separate event also occurs when the backpressure condition ends.
5. Set the **Low BB Credit Threshold**:

**NOTE:** Using default settings for this threshold should work well in most cases. This step is not required.

   This is the percentage of time that the transmitting link cannot transmit because BB_Credit is unavailable. It is the percent of time that the link can be treated as *back-pressured* by the rerouting algorithm. This value is also used when determining routes for a transmit link. A back-pressured ISL cannot be the recipient of traffic rerouted from other ISLs, and traffic on a back-pressured ISL may be rerouted even if the ISL is not congested.
   - Click **Default Threshold** and a default value (1 to 99%) appears in the **Threshold** box. If the default is enabled, you cannot enter values into the box.
   - Click in the threshold box and enter a value from 1 to 99.
6. Click **Activate** to enable these values on the switch and close the dialog box.

## Using the Pop-Up menu

Right-click on columns in the **Congestion Threshold** table to display menu options that globally change values in the column cells. These columns are as follows:

### Use Algorithmic Threshold

Right-click in the column to display these options:

- **Set all to Default**—Adds checks to all check boxes in this column and sets all cells of the **Threshold %** column to default values.
- **Clear All** —Clears all check boxes in this column and restores values in cells of the **Threshold %** column with previous values.

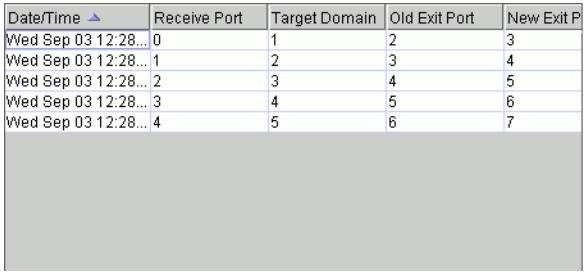
### Threshold %

Right-click in the column to display these options:

- **Set All To xx**—Sets all cells in this column to the value (**xx**) that you clicked.
- **Restore All**— Sets all cells in the column to the previous values.

# Open Trunking log

The Open Trunking log (Figure 73) provides details on flow rerouting that is occurring through switch ports.



| Date/Time | Receive Port | Target Domain | Old Exit Port | New Exit P |
|---|---|---|---|---|
| Wed Sep 03 12:28... | 0 | 1 | 2 | 3 |
| Wed Sep 03 12:28... | 1 | 2 | 3 | 4 |
| Wed Sep 03 12:28... | 2 | 3 | 4 | 5 |
| Wed Sep 03 12:28... | 3 | 4 | 5 | 6 |
| Wed Sep 03 12:28... | 4 | 5 | 6 | 7 |

**Figure 73** Open Trunking log

This log contains the following columns:

- **Date/Time**—Date and time that action occurred.
- **Receive Port**—Decimal receive port number on the local switch associated with the flow that was rerouted.
- **Target Domain**—Decimal domain ID associated with the flow that was rerouted.
- **Old Exit Port**—Decimal exit port number on this switch that the flow used to get to the target domain.
- **New Exit Port**—Decimal exit port number on this switch that the flow now uses to get to the target domain.

# Flexport

Edge Switches can be purchased at a discount with all Fibre Channel ports disabled. The optional Flexport feature is a hardware port expansion kit that lets you upgrade switch capacity on demand in eight-port increments. Flexport kits are available to upgrade the:

- Edge Switch 2/32 from 16 to 24 ports, or from 24 to 32 ports.
- Edge Switch 2/24 from 8 to 16 ports, or from 16 to 24 ports.

Each port expansion kit includes eight SFP optical transceivers and upgrade instructions.

To enable the added port capacity through the Element Manager, a feature key must be purchased and installed through the Configure Feature Key dialog box. There are no other configuration options in HAFM or Element Manager for this feature.

For complete instructions on installing Flexport hardware and upgrading your switch, refer to the *HP StorageWorks Edge Switch 2/24 Flexport upgrade instructions* or the *HP StorageWorks Edge Switch 2/32 Flexport upgrade instructions*.

# A Information and error messages

This appendix lists information and error messages that display in pop-up message boxes from the HP StorageWorks HA-Fabric Manager (HAFM) application and the associated Element Managers.

The first section of the appendix lists HAFM application messages. The second section lists Element Manager messages. The text of each message is followed by a description and recommended course of action.

# HAFM Application messages

Table 7 lists HAFM application information and error messages in alphabetical order.

**Table 7** HAFM messages

| Message | Description | Action |
|---|---|---|
| A zone must have at least one zone member. | When creating a new zone, one or more zone members must be added. | Add one or more zone members to the new zone using the Modify Zone dialog box. |
| A zone set must have at least one zone. | When creating a new zone set, one or more zones must be added. | Add one or more zones to the new zone set using the Modify Zone dialog box. |
| All alias, zone, and zone set names must be unique. | When creating a new alias, zone, or zone set, the name must be unique. | At the New Zone dialog box, select a unique name for the new alias, zone, or zone set. |
| All zone members are logged. | Attempt was made to display all zone members not logged in using the Zone Set tab, but all members are currently logged in. | Informational message. |
| An HAFM application session is already active from this workstation. | Only one instance of the HAFM application is allowed to be open per remote workstation. | Close all but one of the HAFM application sessions. |
| Are you sure you want to delete this network address? | The currently-selected network address will be deleted. | Click **Yes** to delete or **No** to cancel. |
| Are you sure you want to delete this nickname? | The selected nickname will be deleted from the list of nickname definitions. | Click **Yes** to delete the nickname or **No** to cancel the operation. |
| Are you sure you want to delete this product? | The selected product will be deleted from the list of product definitions. | Click **Yes** to delete the product or **No** to cancel the operation. |
| Are you sure you want to delete this user? | The selected user will be deleted from the list of user definitions. | Click **Yes** to delete the user or **No** to cancel the operation. |
| Are you sure you want to delete this zone? | The selected zone will be deleted from the zone library. | Click **Yes** to delete the zone or **No** to cancel the operation. |
| Are you sure you want to delete this zone set? | The selected zone set will be deleted from the zone library. | Click **Yes** to delete the zone set or **No** to cancel the operation. |
| Are you sure you want to overwrite this zone set? | The selected zone set will be overwritten in the zoning library. | Click **Yes** to overwrite or **No** to cancel. |
| Are you sure you want to remove all members from this zone? | All members will be deleted from the selected zone. | Click **Yes** to delete the members or **No** to cancel the operation. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| Cannot add a switch to a zone. | The device that you are attempting to add to the zone is a switch, which cannot be added to a zone. | Specify the port number or corresponding World Wide Name for the device you want to add to the zone. |
| Cannot connect to management server. | The HAFM application at a remote workstation could not connect to the HAFM appliance. | Verify the HAFM appliance internet protocol (IP) address is valid. |
| Cannot delete product. | The selected product cannot be deleted. | Verify the HAFM appliance-to-product link is up.<br>If the link is up:<br>• The HAFM appliance may be busy.<br>• Another Element Manager instance may be open.<br>• You may not have permission to delete the product. |
| Cannot disable Fabric Binding while Enterprise Fabric Mode is active. | You attempted to disable Fabric Binding through the Fabric Binding dialog box, but Enterprise Fabric Mode was enabled. | Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in the HAFM application before disabling Fabric Binding. |
| Cannot display route. All switches in route must be managed by the same server. | You cannot show the route between devices that are attached to switches or directors managed by a different HAFM appliance. | Make sure devices named in Show Routes dialog box are attached to products managed by this HAFM appliance. |
| Cannot display route. All switches in route must support routing. | You cannot show the route through a fabric that has switches or directors which do not support routing. | The route must contain only Edge Switch 2/16s, Edge Switch 2/32s, Director 2/64s, or Director 2/140s. |
| Cannot display route. Device is not a member of a zone in the active zone set. | You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part of a zone in the active zone set. | Enable the default zone or activate the zone for the device before attempting to show the route. |
| Cannot display route on one switch fabric. | You cannot show routes between end devices in a fabric when configuring Show Routes (Configure menu). | Error appears when attempting to show routes on a fabric with only one switch. Configure Show Routes on a multi-switch fabric. |
| Cannot display route. error 9. | An internal error has occurred while trying to view routes. | Contact the next level of support to report the problem. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| Cannot display route. No active zone enabled. | You cannot show the route through a fabric with no active zone. | Enable the default zone or activate a zone set before attempting to show the route. |
| Cannot have spaces in field. | Spaces are not allowed as part of the entry for this box. | Delete spaces from the field entry. |
| Cannot modify a zone set with an invalid name. Rename zone set and try again. | A zone set must have a valid name to be modified. | Assign a valid name to the zone set, then modify the name through the Modify Zone Set dialog box. |
| Cannot modify a zone with an invalid name. Rename zone and try again. | A zone must have a valid name to be modified. | Assign a valid name to the zone, then modify the name through the Modify Zone Set dialog box. |
| Cannot modify product. | The selected product cannot be modified. | Verify the HAFM appliance-to-product link is up. If the link is up:<br>• The HAFM appliance may be busy.<br>• Another Element Manager instance may be open.<br>• You may not have permission to modify the product. |
| Cannot perform operation. Fabric is unknown. | This message appears if no switches in the fabric are connected to the HAFM appliance. | Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM appliance and retry the operation. |
| Cannot perform operation. The list of attached nodes is unavailable. | This message appears when attached nodes are unavailable and you attempt to modify a zone or create a new zone. | Verify an attached node is available and retry the operation. |
| Cannot retrieve current SNMP configuration. | The current SNMP configuration could not be retrieved. | Try again. If the problem persists, contact the next level of support. |
| Cannot save current SNMP configuration. | The current SNMP configuration could not be saved. | Try again. If the problem persists, contact the next level of support. |
| Cannot set write authorization without defining a community name. | An SNMP community name has not been configured. | Enter a valid community name in the Configure SNMP dialog box. |
| Cannot show zoning library. No fabric exists. | You cannot show the zoning library if no fabric exists. You must have identified a switch or director to the *HAFM* application for a fabric to exist. | Identify an existing switch or director to the HAFM application using the New Product dialog box. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| Click OK to remove all contents from log. | This action deletes all contents from the selected log. | Click **OK** to delete the log contents or **Cancel** to cancel the operation. |
| Connection to management server lost. | The connection to the remote HAFM appliance has been lost. | Log in to the HAFM appliance again through the HAFM Log In dialog box. |
| Connection to management server lost. Click OK to exit application. | The HAFM application at a remote workstation lost the network connection to the HAFM appliance. | Re-start the HAFM application to connect to the HAFM appliance. |
| Could not export log to file. | A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected. | If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk. |
| Default zoning is not supported in Open Fabric Mode. | A default zone cannot be enabled when the product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers. | Change the Interop Mode from Open Fabric to Homogeneous using the Configure Fabric Parameters dialog box. You can also redefine zone members by the device WWN. |
| Device is not a member of a zone in the active zone set. | The selected device is not a member of a zone in the active zone set and therefore cannot communicate with the other devices in the route. | Enable the default zone or activate a zone set containing the member before attempting to show the route. |
| Download complete. Click OK and start the HAFM. | Download of HAFM and the Element Manager is complete. | Start the HAFM application to continue. |
| Duplicate community names require identical write authorizations. | If configuring two communities with identical names, they must also have identical write authorizations. | Verify that both communities with the same name have the same write authorizations. |
| Duplicate Fabric Name. | The specified fabric name already exists. | Select another name for the fabric. |
| Duplicate name in zoning configuration. All zone and zone set names must be unique. | Every name in the zoning library must be unique. | Modify (to make it unique) or delete the duplicate name. |
| Duplicate nickname in nickname configuration. | Duplicate nicknames cannot be configured. | Modify the selected nickname to make it unique. |
| Duplicate World Wide Name in nickname configuration. | A World Wide Name can be associated with only one nickname. | Modify (to make it unique) or delete the selected World Wide Name. |
| Duplicate zone in zone set configuration. | More than one instance of a zone is defined in a zone set. | Delete one of the duplicate zones from the zone set. |
| Duplicate zone member in zone configuration. | More than one instance of a zone member is defined in a zone. | Delete one of the duplicate zone members from the zone. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| Element Manager instance is currently open. | A product cannot be deleted while an instance of the Element Manager is open for that product. | Close the Element Manager, then delete the product. |
| Enabling this zone set will replace the currently active zone set. Do you want to continue? | Only one zone set can be active. By enabling the selected zone set, the current active zone set will be replaced. | Click **OK** to continue or **Cancel** to end the operation. |
| Error connecting to switch. | While viewing routes, the HAFM appliance was unable to connect to the switch. The switch failed or the switch-to-HAFM appliance Ethernet link failed. | Try the operation again. If the problem persists, contact the next level of support. |
| Error creating zone. | The HAFM application encountered an internal error. | Try the operation again. If the problem persists, contact the next level of support. |
| Error creating zone set. | The HAFM application encountered an internal error. | Try the operation again. If the problem persists, contact the next level of support. |
| Error deleting zone. | The HAFM application encountered an internal error. | Try the operation again. If the problem persists, contact the next level of support. |
| Error deleting zone set. | The HAFM application encountered an internal error. | Try the operation again. If the problem persists, contact the next level of support. |
| Error reading log file. | The HAFM application encountered an error while trying to read the log. | Try the operation again. If the problem persists, contact the next level of support. |
| Error removing zone or zone member. | The HAFM application encountered an internal error. | Try the operation again. If the problem persists, contact the next level of support. |
| Error transferring files < message >. | An error occurred while transferring files from the PC hard drive to the HAFM application. The message varies, depending on the problem. | Try the file transfer operation again. If the problem persists, contact the next level of support. |
| Fabric Log will be lost once the fabric unpersists. Do you want to continue? | When you unpersist a fabric, the corresponding fabric log is deleted. | Click **Yes** to unpersist the fabric or **No** to cancel the operation. |
| Fabric member could not be found. | A fabric member does not exist when the application prepared to find a route, find a route node, or gather route information on that fabric member. | Ensure the product is incorporated into the fabric and retry the operation. If the problem persists, contact the next level of support. |
| Fabric not persisted. | You attempted to refresh or clear the log, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted. | Click **OK** to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log. |
| Field cannot be blank. | The data field requires an entry and cannot be left blank. | Enter appropriate information in the data field. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| File transfer aborted. | You aborted the file transfer process. | Verify the file transfer is to be aborted, then click **OK** to continue. |
| HAFM error <error number 1 through 8 >. | The HAFM application encountered an internal error (1 through 8 inclusive) and cannot continue operation. | Contact the next level of support to report the problem. |
| Management server could not log you on. Verify your username and password. | An incorrect username or password (both case sensitive) was used while attempting to log in to the HAFM application. | Verify the username and password with the customer's network administrator and retry the operation. |
| Management server is shutting down. Connection will be terminated. | The HAFM application is closing and terminating communication with the attached product. | Reboot the HAFM appliance. If the problem persists, contact the next level of support. |
| Invalid character in field. | An invalid character was entered in the data field. | Remove invalid characters from the entry. |
| Invalid name. | One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN. | Select a valid name and retry the operation. |
| Invalid network address. | The IP address specified for the product is unknown to the domain name server (invalid). | Verify and enter a valid product IP address. |
| Invalid port number. Valid ports are (0-< nn >). | You have specified an invalid port number. | Specify a valid port number, in the range 0 to the maximum number of ports on the product minus 1. For example, for a switch with 32 ports, the valid port range is 0–31. |
| Invalid product selection. | At the New Product dialog box, an invalid product was selected. | Select a valid product and retry the operation. |
| Invalid request. | Three conditions result in this message:<br>• You tried to add or modify a product from **Product View** and the network address is already in use. (Network addresses must be unique.)<br>• You tried to create a new user with a username that already exists. (A username must be unique.)<br>• You tried to delete the default Administrator user. (The default Administrator user cannot be deleted.) | Select the action that is appropriate to the activity that caused the error:<br>• Network address: Specify a unique network address for the product.<br>• username: Specify a unique username for the new user ID.<br>• Do not delete the default Administrator user. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| Invalid UDP port number. | The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive. | Verify and enter a valid UDP port number. |
| Invalid World Wide Name. | The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx: xx:xx:xx:xx). | Enter a World Wide Name using the correct format. |
| Invalid World Wide Name or nickname. | The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx: xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters. | Try the operation again using a valid World Wide Name or nickname. |
| Invalid World Wide Name. Valid WWN format is: xx:xx:xx:xx:xx: xx:xx:xx. | The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx: xx:xx:xx:xx). | Retry the operation using a valid WWN or nickname. |
| Invalid zone in zone set. | The defined zone no longer exists and is invalid. | Delete the invalid zone from the zone set. |
| Limit exceeded. | You cannot add a new product or user to HAFM application if the maximum number of that resource already exists on the system. | Delete unneeded products or users from the system, before attempting to add any new ones. |
| No address selected. | You cannot complete the operation because an address has not been selected. | Select an address and retry the operation. |
| No attached nodes selected. | An operation was attempted without an attached node selected. | Select an attached node and try the operation again. |
| No management server specified. | An HAFM appliance is not defined to the HAFM application. | At the HAFM 8 Log In dialog box, type an appliance name in the **Server Name** field and click **Login**. |
| No nickname selected. | No nickname was selected when the command was attempted. | Select a nickname and try again. |
| No Element Managers installed. | No director or switch Element Manager is installed on this workstation. | Install the appropriate Element Manager to this workstation. |
| No routing information available. | No information is available for the route selected. | Select a different route and try the operation again. |
| No user selected. | A user was not selected when the command was attempted. | Select a user and try again. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| No zone member selected. | A zoning operation was attempted without a zone member selected. | Select a zone member and try the operation again. |
| No zone selected. | A zoning operation was attempted without a zone selected. | Select a zone and try the operation again. |
| No zone selected or zone no longer exists. | A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric. | Select a zone and try the operation again. |
| No zone set active. | A zone set cannot be deactivated if there are no active zones. | Informational message only—no action is required. |
| No zone set selected. | A zoning operation was attempted without a zone set selected. | Select a zone set and try the operation again. |
| No zone set selected or zone set no longer exists. | A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric. | Select a zone set and try the operation again. |
| Only attached nodes can be displayed in this mode. | You cannot display unused ports when adding ports by World Wide Name. | Change the add criteria to Add by Port. |
| Password and confirmation don't match. | Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same. | Enter the password and confirmation password again. |
| Remote sessions are not allowed from this network address. | Only IP addresses of remote workstations specified at the Remote Access dialog box are allowed to connect to the HAFM appliance. | Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions. |
| Remote session support has been disabled. | The connection between the specified remote workstation and the HAFM appliance was disallowed. | Consult with the customer's network administrator to determine if the workstation entry should be modified at the Remote Access dialog box. |
| Resource is unavailable. | The specified operation cannot be performed because the product is unavailable. | Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later. |
| Route data corrupted. | The information for this route is corrupt. | Try the operation again. If the problem persists, contact the next level of support. |
| Route request timeout. | The Show Route request timed out. | Try the operation again. If the problem persists, contact the next level of support. |
| Routing is not supported by the switch. | This switch or director does not support the Show Routes feature. | Select a different switch or director to show the route. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| SANtegrity Feature not installed. Please contact your sales representative. | You selected **Fabric Binding** or **Enterprise Fabric Mode** from the Fabrics menu. These selections are not enabled because the optional SANtegrity binding feature is not installed. | Install the SANtegrity Binding feature to use Fabric Binding or enable Enterprise Fabric Mode. |
| Select alias to add to zone. | An alias was not selected before clicking **Add**. | Select an alias before clicking **Add**. |
| Selection is not a World Wide Name. | The selection made is not a World Wide Name. | Select a valid World Wide Name before performing this operation. |
| Server shutting down. | The HAFM application is closing and terminating communication with the attached product. | Reboot the HAFM appliance. If the problem persists, contact the next level of support. |
| SNMP trap address not defined. | If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined. | Enter a corresponding SNMP trap recipient address. |
| Switch is not managed by HAFM. | The selected switch or director is not managed by the HAFM application. | Select a different switch or director. |
| The Administrator user cannot be deleted. | The administrator user is permanent and cannot be deleted from the Configure Users dialog box. | Informational message only—no action is required. |
| The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List. | You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but a switch already exists in the fabric with the same domain ID. | Enter a unique domain ID for the switch in the Add Detached Switch dialog box. |
| The management server is busy processing a request from another Element Manager. | The HAFM appliance is processing a request from another instance of an Element Manager and cannot perform the requested operation. | Wait until the process completes, then perform the operation again. |
| The link to the managed product is not available. | The Ethernet connection between the HAFM appliance and managed product is down or unavailable. | Establish and verify the network connection. |
| The maximum number of aliases has already been configured. | The maximum number of aliases allowed was reached. | Delete an existing alias before adding a new alias. |
| The maximum number of management server network addresses has already been configured. | The number of HAFM appliance IP addressees that can be defined to the HAFM application has already been configured. | Delete an existing IP address before adding a new address. |
| The maximum number of members has already been configured. | The maximum number of unique members is 4097. The maximum number of members is 8192. | Delete an existing zone member before adding a new zone member. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| The maximum number of nicknames has already been configured. | The maximum number of nicknames that can be defined to the HAFM application was reached. | Delete an existing nickname before adding a new nickname. |
| The maximum number of open products has already been reached. | The maximum number of open switches allowed was reached. | Close an Element Manager session (existing open product) before opening a new session. |
| The maximum number of products has already been configured. | The number of managed HP switches (48) that can be defined to the HAFM application was reached. | Delete an existing product before adding a new product. |
| The maximum number of products of this type has already been configured. | The number of managed HP switches of this type (48) that can be defined to the HAFM application was reached. | Delete an existing product of this type before adding a new product. |
| The maximum number of remote network addresses has already been configured. | A maximum number of eight IP addresses for remote workstations can be configured at the Session Options dialog box. That number was reached. | Delete an existing IP address before adding a new IP address. |
| The maximum number of users has already been configured. | The number of users (32) that can be defined to the HAFM application was reached. | Delete an existing user before adding a new user. |
| The maximum number of zones allowed has already been configured. | The maximum number of zones that can be defined was reached. | Delete an existing zone before adding a new zone. |
| The maximum number of zone sets has already been configured. | The maximum number of zone sets that can be defined was reached. | Delete an existing zone set before adding a new zone set. |
| The maximum number of zones per zone set has already been configured. | The maximum number of zones that can be defined in a zone set was reached. | Delete an existing zone before adding a new zone to the zone set. |
| The nickname does not exist. | The entered nickname does not exist in the fabric. | Configure the nickname to the appropriate product or select an existing nickname. |
| The nickname is already assigned. Either use a different name or do not save the name as a nickname. | The entered nickname already exists in the fabric. Each nickname must be unique. | Define a different nickname. |
| The software version on this management server is not compatible with the version on the remote management server. | A second HAFM appliance (client) connecting to the HAFM appliance must be running the same software version to log in. | Upgrade the software version on the downlevel HAFM appliance. |
| The zoning library conversion must be completed before continuing. | The zoning library conversion is incomplete and the requested operation cannot continue. | Complete the zoning library conversion, then retry the operation. |
| This fabric log is no longer valid because the fabric has been unpersisted. | The selected fabric log is no longer available because the fabric has been unpersisted. | To start a new log for the fabric, persist the fabric through the Persist Fabric dialog box. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| This network address has already been assigned. | The specified IP address was assigned and configured. A unique address must be assigned. | Consult with the customer's network administrator to determine a new IP address to be assigned and configured. |
| This product is not managed by this management server. | The product selected is not managed by this HAFM appliance. | Select a product managed by this HAFM appliance or go to the HAFM appliance that manages the affected product. |
| This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List. | You attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric. | Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected. |
| This World Wide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List. | You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but an entry already exists in the Fabric Membership List with the same World Wide Name (WWN). | Enter a unique World Wide Name for the switch in the Add Detached Switch dialog box. |
| Too many members defined. | The maximum number of zone members that can be defined was reached. | Delete an existing zone member before adding a new zone member. |
| You do not have a compatible version of the management server software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click OK to install a compatible version. | The HAFM application version running on the HAFM appliance differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM appliance. | Download a compatible version of the HAFM application to the remote workstation (client) using the Web install procedure. |
| You do not have rights to perform this action. | Configured user rights do not allow this operation to be performed. | Verify user rights with the customer's network administrator and change as required using the Configure Users dialog box. |
| You must define an SMTP server address. | An SMTP server address must be defined and configured for e-mail to be activated. | Define the SMTP server address at the Configure E-Mail dialog box. |
| You must define at least one E-mail address. | At least one e-mail address must be defined and configured for e-mail to be activated. | Define an e-mail address at the Configure E-Mail dialog box. |

**Table 7** HAFM messages (continued)

| Message | Description | Action |
|---|---|---|
| You must define at least one remote network address. | At least one IP address for a remote workstation must be configured for a remote session to be activated. | Define an IP address for at least one remote workstation at the Remote Access dialog box. |
| You must download the HAFM client via the web install. | An attempt was made to download the HAFM application to a remote workstation (client) using an improper procedure. | Download a compatible version of the HAFM application to the remote workstation (client) using the Web install procedure. |
| Zones configured with port numbers are ignored in Open Fabric Mode. | While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names. | Informational message only–no action is required. |
| Zones must be defined before creating a zone set. | You cannot create a zone set without any zones defined for HAFM. | Define zones using the New Zone dialog box. |
| Zoning by port number is ignored in Open Fabric Mode. | While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names. | Informational message only–no action is required. |
| Zoning by port number is not supported in Open Fabric Mode. | You cannot specify an item for zoning by port number if HAFM is in Open Fabric Mode. | Either define zones by WWN of device or change to Homogeneous Fabric mode in the Configure Operation Mode dialog box of the Element Manager. |
| Zoning name already exists. | Duplicate zone names are not allowed in the zoning library. | Modify (to make it unique) or delete the duplicate zone name. |

# Element Manager messages

Table 8 lists Element Manager information and error messages in alphabetical order

**Table 8** Element Manager messages

| Message | Description | Action |
|---|---|---|
| A Preferred Path already exists between this Source Port and this Destination Domain ID. Please re-configure the desired path. | For any source port, only one path may be defined to each destination domain ID. | On the Add/Change Preferred Path dialog box, change the preferred path. |
| Activating this configuration will overwrite the current configuration. | Confirmation to activate a new address configuration. | Click **Yes** to confirm activating the new address configuration or **No** to cancel the operation. |
| All configuration names must be unique. | All address configurations must be saved with unique names. | Save the configuration with a different name that is unique to all saved configurations. |
| All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue? | Occurs when FPM cards are installed in the director and director speed is being set to 2 Gb/sec in the Configure Switch Parameters dialog box. | Replace FPM cards with UPM cards (UPM cards operate at 1 and 2 Gb/sec) or set the director speed to 1 Gb/sec. |
| All port names must be unique. | A duplicate Fibre Channel port name was configured. All port names must be unique. | Reconfigure the Fibre Channel port with a unique name. |
| All port names must be unique. | A duplicate port name was entered. Every configured port name must be unique. | Reconfigure the port with a unique name. |
| An Element Manager instance is already open. | Only one instance of the Element Manager can be open at one time. | Close the open Element Manager so the desired instance of the Element Manager can be opened. |
| Another Element Manager is currently performing a firmware install. | Only one instance of the Element Manager can install a firmware version to the director at a time. | Wait for the firmware installation process to complete and try the operation again. |
| Are you sure you want to delete firmware version? | This message requests confirmation to delete a firmware version. Firmware library can store up to 8 firmware versions. | Click **Yes** to delete the firmware version or **No** to abort the operation. |
| Are you sure you want to delete this address configuration? | Confirmation to delete the selected address configuration. | Click **Yes** to confirm the deletion of the address configuration or **No** to cancel the operation. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Are you sure you want to send firmware version? | This message requests confirmation to send a firmware version from the HAFM appliance's firmware library to the director. Firmware library can store up to 8 firmware versions. | Click **Yes** to send the firmware version or **No** to abort the operation. |
| Cannot change Port Type while Management Style is FICON without SANtegrity feature. Please contact your sales representative. | Firmware is below the required level and you attempted to change a port type in the Configure Ports dialog box while FICON management style, but the optional SANtegrity Binding feature is not installed. | Informational message. If the firmware is below the required level, install SANtegrity Binding before changing port types in the Configure Ports dialog box while in FICON management style. |
| Cannot create partition <partition_number> while FICON Management Server is enabled. | The user has moved slots into a partition while FMS Server is enabled. | Disable FMS Server before moving slots into a partition. |
| Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online. | You attempted to disable Switch Binding through the Switch Binding Change State dialog box, but Enterprise Fabric Mode is enabled. | You must either disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the **HAFM** application or set the switch offline before you can disable Switch Binding. |
| Cannot disable Insistent Domain ID while Fabric Binding is active. | You attempted to disable the Insistent Domain ID parameter through the Configure Switch Parameters dialog box, but Fabric Binding is enabled. | Disable Fabric Binding through the Fabric Binding dialog box before disabling these parameters. |
| Cannot enable beaconing on a failed FRU. | Occurs when selecting Enable Beaconing option for a failed FRU. | Replace FRU and enable beaconing again or enable beaconing on operating FRU. |
| Cannot enable beaconing while the system light is on. | Occurs when choosing Enable Beaconing option for a failed FRU. | Replace FRU and enable beaconing again or enable beaconing on an operating FRU. |
| Cannot enable beaconing while the system error light is on. | Beaconing cannot be enabled while the system error light is on. | Select **Clear System Error Light** from **Product** menu to clear error light, then enable beaconing. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Cannot enable Open Trunking while Enterprise Fabric Mode is active and the switch is offline. | Enterprise Fabric mode is active and the switch or director is online and you attempted to enable Open Trunking. This message only appears if the optional Open Trunking feature is installed. | Perform either of the following steps:<br>Disable Enterprise Fabric Mode option by selecting the appropriate fabric in the Fabric Tree portion of the HAFM Manager window (Fabrics tab) and then selecting **Enterprise Fabric Mode** from the Fabrics menu. When the Enterprise Fabric Mode dialog box appears, click **Start** and follow prompts to disable the feature.<br>Set the switch or director offline through the Set Online State dialog box. Display this dialog box by selecting **Set Online State** from the Element Manager Maintenance menu. |
| Cannot have E-Ports if Management Style is FICON unless SANtegrity feature is installed. Please contact your sales representative. | Firmware is below the required level and you attempted to change management style from Open Systems to FICON management style with E_Ports configured, but SANtegrity Binding is not installed. | Informational message. If firmware is below the required level and you install SANtegrity Binding before changing to FICON management style, then E_Ports will remain as E_Ports when you change to FICON management style. If SANtegrity Binding is not installed, setting a director to FICON management style will change all E_ports to G_Ports. |
| Cannot have spaces in field. | Spaces are not allowed as part of the entry for this field. | Delete spaces from the field entry. |
| Cannot install firmware to a director with a failed CTP card. | A firmware version cannot be installed on a director with a failed control processor (CTP) card. | Replace the failed CTP card and retry the firmware installation. |
| Cannot install firmware to a switch with a failed CTP card. | Firmware cannot be installed on a switch with a defective CTP card. | Note that the CTP card is not a FRU. If it fails, the switch must be replaced. After replacement, retry the firmware install to the switch. |
| Cannot modify director/switch speed. Ports speeds cannot be configured at a higher data rate than the director/switch speed. | Port speeds cannot be configured at a higher data rate than the director speed. This message appears when you set director sped to 1 GB/sec through the Configure Switch Parameters dialog box and at least one of the ports is running at 2 Gb/sec. | Either return the director speed to 2 Gb/sec or configure all port data speeds to 1 Gb/sec through the Configure Ports dialog box. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Cannot perform this operation while the switch is offline. | This operation cannot take place while the director or switch is offline. | Configure the director or switch offline through the Set Offline State dialog box and then retry the operation. |
| Cannot retrieve current SNMP configuration. | The director SNMP configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot retrieve diagnostics results. | Director diagnostic results cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot retrieve information for port. | Port information cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot retrieve port configuration. | The port configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot retrieve port statistics. | Port statistics cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot retrieve switch date and time. | The director or switch date and time cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot retrieve switch state. | The director or switch state cannot be retrieved by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot run diagnostics on a port that is failed. | Port diagnostics (loopback tests) cannot be performed on a port that has failed any previous diagnostic (power-on diagnostic, online diagnostic, or loopback test). The amber LED associated with the port illuminates to indicate the failed state. | Reset the port and perform diagnostics again. |
| Cannot run diagnostics on an active E-port. | Port diagnostics cannot be performed on an active E-port. | Run diagnostics on an E-port only when it is not active. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Cannot run diagnostics on a port that is not installed. | Port diagnostics cannot be performed on a port card that is not installed. | Run diagnostics only on a port that is installed. |
| Cannot run diagnostics on a port card that is not installed. | Port diagnostics (loopback tests) cannot be performed on a port that does not have a small form factor (SFF) optical transceiver installed. | Install a transceiver in the port and perform diagnostics again. |
| Cannot run diagnostics while a device is logged-in to the port. | Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in. | Ensure the device is logged out and perform diagnostics again. |
| Cannot run diagnostics while a device is logged-in to the port. | A device is logged in to the port where a diagnostic test is attempted. | Log out the device and run the diagnostic test again. |
| Cannot save IPL configuration while active=saved is enabled. | You cannot save the IPL file while the active=saved property is set. | The FICON Management Server property, active=save, must be disabled for HAFM to save the IPL file. |
| Cannot save port configuration. | The port configuration cannot be saved at the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot save SNMP configuration. | The SNMP configuration cannot be saved at the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot set all ports to 1 Gb/sec due to speed restriction on some ports. | Appears if you try to set ports to operate at 1 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration. | Replace ports that do not support speed configuration with those that do support more than one configuration. |
| Cannot set all ports to 2 Gb/sec due to speed restriction on some ports. | Appears if you try to set ports to operate at 2 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration. | Replace ports that do not support speed configuration with those that do support more than one configuration. |
| Cannot set all ports to Negotiate due to port speed restriction on some ports. | Appears if you try to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration. | Replace ports that do not support speed configuration with those that do support more than one speed configuration. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Cannot set Fibre Channel parameters. | Fibre Channel parameters for the director cannot be set at the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot set switch date and time. | The switch date and time cannot be set at the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot set switch state. | The director or switch state cannot be set at the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot set write authorization without defining a community name. | A community name was not defined in the Configure SNMP dialog box for the write authorization selected. | Provide a name in the **Name** field where write authorization is checked. |
| Cannot start data collection. | The data collection procedure cannot be started by the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot start firmware install while CTP synchronization is in progress. | The director's CTP cards are synchronizing and firmware cannot be installed until synchronization is complete. | Install the firmware after CTP card synchronization completes. |
| Cannot start port diagnostics. | Port diagnostics cannot be started at the Element Manager because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Cannot swap an uninstalled port. | A port swap cannot be performed when the port card is not installed. | Perform a swap only on a port that is installed. |
| Click OK to remove all contents from log. | This action deletes all contents from the selected log. | Click **OK** to delete the log contents or click **Cancel** to cancel the operation. |
| Connection to management server lost. Click OK to exit application. | The *HAFM* application at a remote workstation lost the network connection to the HAFM appliance. | Start the *HAFM* application to connect to the HAFM appliance. |
| Continuing may overwrite host programming. Continue? | Configurations sent from the host may be overwritten by HAFM. | Continuing will activate the current configuration, which may have been configured by a FICON host. |
| Could not export log to file. | A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected. | Ensure file name and drive are correct. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Could not find firmware file. | Firmware file selected was not found in the FTP directory. Or, the selected file is not a firmware file. | Ensure file name and directory are correct. Or, obtain a valid firmware file from your service representative. |
| Could not remove dump files from server. | Dump files could not be deleted from the HAFM appliance because the link may be down, or the HAFM appliance or Element Manager is busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Could not stop port diagnostics. | Port diagnostics could not be stopped by the Element Manager because the Ethernet link is down or busy, or because the director is busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Could not write firmware to flash. | A firmware version could not be written from the HAFM appliance to FLASH memory | Retry the operation again. If the condition persists, contact the next level of support. |
| Control Unit Port (CUP) name and port name are identical (FICON ONLY). | Within the address configuration, one or more of the port names are the same as the CUP name. | Make sure all names are unique for the ports and CUP name. |
| Date entered is invalid. | The date is entered incorrectly at the Configure Date and Time dialog box. Individual field entries may be correct, but the overall date is invalid (for example, a day entry of 31 for a 30-day month). | Verify each entry is valid and consistent. |
| Device applications should be terminated before starting diagnostics. Press **NEXT** to continue. | Port diagnostics (loopback tests) cannot be performed on a port while an attached device application is running. | Terminate the device application and perform diagnostics again. |
| [device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed. | You attempted to remove a device WWN from the Switch Membership List (SANtegrity Binding feature) while Switch Binding is enabled. | Remove the device from the switch by blocking the port, setting the switch offline, or disabling Switch Binding through the Switch Binding Change State dialog box before removing devices from the Switch Membership List. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Director clock alert mode must be cleared before enabling period synchronization. | Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box. | Disable clock alert mode through the Configure FICON Management Server dialog box. |
| Director must be offline to configure. | Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box. | Disable clock alert mode through the Configure FICON Management Server dialog box. |
| Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue? | Fabric Binding is enabled through HAFM and you attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box. | Click **Yes** if you want to continue and disable Fabric Binding. |
| Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue? | Fabric Binding is enabled through the HAFM and user attempted to disable Insistent Domain ID in the **Configure Switch Parameters** dialog box. | Click **Yes** if you want to continue and disable Fabric Binding. |
| Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue? | You attempted to disable Switch Binding through the Switch Binding State Change dialog box, but Enterprise Fabric Mode is enabled. | Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Switch Binding. |
| Do you want to continue with IPL? | This message requests confirmation to initial program load (IPL) the director. | Click **Yes** to IPL the director or **Cancel** to cancel the operation. |
| Domain IDs must be in the range of 1 to 31. | Domain IDs entered in the Configure Preferred Paths dialog box must fall in a specific range. | In the Configure Preferred Paths dialog box, change the number in the **Destination Domain ID** field to a number between 1 and 31, inclusive. |
| Duplicate Community names require identical write authorizations. | Duplicate community names are entered at the Configure SNMP dialog box, and have different write authorizations. | Delete the duplicate community name or make the write authorizations consistent. |
| Element Manager error <number>. | The Element Manager encountered an internal error and cannot continue. | Contact the next level of support to report the problem. |
| Element Manager instance is currently open. | A Element Manager window is currently open. | Informational message only. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCNs. Do you want to continue? | You attempted to disable these parameters in the Configure Switch Parameters dialog box while the switch was online, but Enterprise Fabric Mode (SANtegrity Binding feature) is enabled. | Click **Yes** if you want to continue, and disable Enterprise Fabric Mode. |
| Error retrieving port information. | An error occurred at the Element Manager while retrieving port information because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Error retrieving port statistics. | An error occurred at the Element Manager while retrieving port statistics because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Error stopping port diagnostics. | An error occurred at the Element Manager while attempting to stop port diagnostics from running because the Ethernet link is down or busy. | Retry the operation later. If the condition persists, contact the next level of support. |
| Error transferring files < message >. | An error occurred while transferring files from the PC hard drive to the Element Manager. The message varies, depending on the problem. | Try the file transfer operation again. If the problem persists, contact the next level of support. |
| Feature not supported. The 'product name' must be running version 05.00.00 or higher. | The firmware version on the hardware product (switch or director) is lower than 05.00.00. This message only appears if the optional Open Trunking feature is installed. | Install firmware version 5.00.00 or higher on the hardware product. |
| Field cannot be blank. | The data field requires an entry and cannot be left blank. | Enter appropriate information in the Data field. |
| Field has exceeded maximum number of characters. | The maximum number of data entry characters allowed in the field was exceeded. | Enter the information using the prescribed number of characters. |
| File transfer aborted. | You aborted the file transfer process. | Information message only. |
| File transfer is in progress. | A firmware file is being transferred from the HAFM appliance hard drive, or a data collection file is being transferred to a CD. | Informational message only—no action is required. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Firmware download timed out. | The director or switch did not respond in the time allowed. The status of the firmware install operation is unknown. | Retry the operation. If the problem persists, contact the next level of support. |
| Firmware file I/O error. | A firmware download operation aborted because a file I/O error occurred. | Retry the operation. If the problem persists, contact the next level of support. |
| Firmware file not found. | The firmware version is not installed (or was deleted) from the firmware library at the HAFM appliance. | Add the firmware version to the library and retry the operation. |
| Incompatible configuration between management style and management server. | If the Firmware is below the required level, only FICON management style is allowed if the FICON Management Server feature is enabled. You attempted to enable Open Systems management style. | Disable FICON Management Server, enable the Open Systems Management Server, or enable the Open Systems management style. |
| Incorrect product type. | When configuring a new product through the New Product dialog box, an incorrect product was specified. | Select the correct product type for the product with the network address. |
| Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key? | If the switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM appliance will be lost momentarily, but Fibre Channel traffic will not be affected. | Click **Yes** to install the feature key or **No** to not install. |
| Internal file transfer error received from director. | The director or switch detected an internal file transfer error. | Retry the operation. If the problem persists, contact the next level of support. |
| Invalid character in field. | An invalid character was entered in the Data field. | Remove invalid characters from the entry. |
| Invalid configuration name. | Attempted to save an address configuration name with an invalid name. | Use up to 24 alphanumeric characters, including spaces, hyphens, and underscores. |
| Invalid feature key. | The feature key was not recognized. | Re-enter the feature key. Ensure that you type each character in the correct case (upper or lower), include the dashes, and do not add any spaces at the end. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Invalid firmware file. | The file selected for firmware download is not a firmware version file. | Select the correct firmware version file and retry the operation. |
| Invalid management server address. | The IP address specified for the HAFM appliance is unknown to the domain name server (invalid). | Verify and enter a valid HAFM appliance IP address. |
| Invalid network address. | The IP address specified for the product is unknown to the domain name server (invalid). | Verify and enter a valid product IP address. |
| Invalid port address. | Invalid port address has been entered. | Verify port address through the Configure Addresses–"Active" dialog box (FICON management style only) and re-enter. |
| Invalid port number. | The port number must be within a range of ports for the specific director or switch model. | Enter a port number within the correct range. |
| Invalid port swap. | Port swap selection is not allowed. | Ensure that each port selected for swap has not been previously swapped. |
| Invalid response received from switch. | An error occurred at the switch during a firmware download operation. | Retry the firmware download operation. If the problem persists, contact the next level of support. |
| Invalid response received from director. | An error occurred at the director during a firmware download operation. | Retry the firmware download operation. If the problem persists, contact the next level of support. |
| Invalid serial number for this feature key. | The serial number and the feature key did not match. | Ensure that the feature key being installed is specifically for this director serial number. |
| Invalid UDP port number. | The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive. | Verify and enter a valid UDP port number from 1 through 655535. |
| Invalid value for BB_Credit. | At the Configure Fabric Parameters dialog box, the buffer-to-buffer credit (BB_Credit) value must be an integer from 1 through 60 inclusive. | Verify and enter a valid number between 1 through 60. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Invalid value for Low BB Credit threshold (1-99) %. | Low BB Credit Threshold field in Configure Open Trunking dialog box must have entries in the range from 1 and 99. This message only appears if the optional Open Trunking feature is installed. | Enter a value from 1 to 99 into the Low BB Credit Threshold field of the Configure Open Trunking dialog box. |
| Invalid value for day (1-31). | At the Configure Date and Time dialog box, the DD value (day) must be an integer from 1 through 31 inclusive. | Verify and enter a valid date. |
| Invalid value for E_D_TOV. | At the Configure Fabric Parameters dialog box, the error detect time-out value (E_D_TOV) must be an integer from 2 through 600 inclusive. | Verify and enter a valid number. |
| Invalid value for hour (0-23). | At the Configure Date and Time dialog box, the HH value (hour) must be an integer from 0 through 23 inclusive. | Verify and enter a valid time. |
| Invalid value for minute (0-59). | At the Configure Date and Time dialog box, the MM value (minute) must be an integer from 0 through 59 inclusive. | Verify and enter a valid time. |
| Invalid value for month (1-12). | At the Configure Date and Time dialog box, the MM value (month) must be an integer from 1 through 12 inclusive. | Verify and enter a valid date. |
| Invalid value for R_A_TOV. | At the Configure Fabric Parameters dialog box, the resource allocation time-out value (R_A_TOV) must be an integer from 10 through 1200 inclusive. | Verify and enter a valid number. |
| Invalid value for second (0-59). | At the Configure Date and Time dialog box, the SS value (second) must be an integer from 0 through 59 inclusive. | Verify and enter a valid time. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Invalid value for threshold (1-99)%. | Value entered for each port in the Configure Open Trunking dialog box must be in the range from 1 to 99. This message only appears if the optional Open Trunking feature is installed. | Enter a number from 1 to 99 into the **Threshold %** column of the Configure Open Trunking dialog box. |
| Invalid value for year. | At the Configure Date and Time dialog box, the YYYY value (year) must be a four-digit value. | Verify and enter a four-digit value for the year. |
| Invalid World Wide Name or nickname. | The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx: xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters. | Try the operation again using a valid World Wide Name or nickname. |
| Link dropped. | The HAFM appliance-to-director Ethernet link was dropped. | Retry the operation. Link re-connects are attempted every 30 seconds. If the condition persists, contact the next level of support. |
| Log is currently in use. | Access to the log is denied because the log was opened by another instance of the Element Manager. | Retry the operation later. If the condition persists, contact the next level of support. |
| Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue. | External loopback diagnostics require an optical loopback plug to be installed. | Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing. |
| Maximum number of versions already installed. | The number of firmware versions that can be defined to the HAFM application's firmware library (eight) was reached. | Delete an existing firmware version before adding a new version. |
| No file was selected. | Action requires the selection of a file. | Select a file. |
| No firmware version file was selected. | A file was not selected in the Firmware Library dialog box before an action, such as modify or send was performed. | Click on a firmware version in the dialog box to select it, then perform the action again. |
| No firmware versions to delete. | There are no firmware versions in the firmware library to delete, therefore the operation cannot be performed. | Informational message only—no action is required. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Nonredundant director must be offline to install firmware. | For directors, if the director has only one CTP card, the director must be set offline to install a firmware version.<br>For switches, since the switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU. | Set the director or switch offline and install the firmware. |
| Not all of the optical transceivers are installed for this range of ports. | Some ports in the specified range do not have optical transceivers installed. | Use a port range that is valid for the ports installed. |
| Open Trunking is not installed for this product. Please contact your sales representative. | The Open Trunking feature key has not been enabled. This message only appears if the optional Open Trunking feature is installed. | Enter the feature key into the Configure Feature Key dialog box and enable the key. If you require a feature key, see your account representative. |
| Performing this operation will change the current state to Offline. | This message requests confirmation to set the director offline. | Click **OK** to set the director offline or click **Cancel** to cancel the operation. |
| Performing this operation will change the current state to Online. | This message requests confirmation to set the director online. | Click **OK** to set the director online or click **Cancel** to cancel the operation. |
| Performing this action will overwrite the date/time on the switch. | Warning that occurs when configuring the date and time through the Configure Date and Time dialog box, that the new time or date will overwrite the existing time or date set for the director or switch. | Verify that you want to overwrite the current date or time. |
| Periodic Date/Time synchronization must be cleared. | Action cannot be performed because Periodic Date/Time Synchronization option is active. | Click **Periodic Date/Time Synchronization** check box in Configure Date and Time dialog box (Configure menu) to clear check mark and disable periodic date/time synchronization. |
| Port binding was removed from attached devices that are also participating in Switch Binding. | Informational message. You removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding. | Review the Switch Binding Membership List to determine if the devices should be members. |
| Port cannot swap to itself. | Port addresses entered in the Swap Ports dialog box are the same. | Ensure that address in the first and second Port Address fields are different. |
| Port diagnostics cannot be performed on an inactive port. | This appears when port diagnostics is run on a port in an inactive state. | Run the diagnostics on an active port. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Port speeds cannot be configured at a higher rate than the director speed. | This appears when you configure a port to 2 Gb/sec and the director speed is set to 1 Gb/sec. | Set the director speed to 2 Gb/sec in the Configure Switch Parameter dialog box. |
| Port numbers must be in the range of 0 to xxx. | When configuring Preferred Paths, source ports and exit ports must be in the range of ports for the switch being configured. | In the Configure Preferred Paths dialog box, change the numbers in the **Source Port** and **Exit Port** fields to fall within the port count of the switch on which you are configuring paths. |
| Preferred Paths can not be enabled until the Domain ID is set to Insistent. Disable Preferred Paths, then configure Switch Parameters. | If the switch's domain ID has not been set to Insistent, the user is not allowed to activate the Preferred Path configuration with the Enable Preferred Paths check box selected. | Close the Configure Preferred Paths dialog box and click **Configure** > **Operating Parameters** > **Switch Parameters**. In the Configure Switch Parameters dialog box, click the **Insistent** check box. |
| R_A_TOV must be greater than E_D_TOV. | R_A_TOV must be greater than E_D_TOV. | Change one of the values so that R_A_TOV is greater than E_D_TOV |
| Resource is unavailable. | The specified operation cannot be performed because the product is unavailable. | Verify that the Ethernet connection between the HAFM appliance and the director is up or available. |
| Resource is unavailable. | The specified operation cannot be performed because the product is unavailable. | Verify that the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later. |
| SANtegrity Feature not installed. Please contact your sales representative. | You selected **Switch Binding** from the Configure menu, but the optional SANtegrity Binding feature is not installed. | Install the SANtegrity Binding key through the Configure Feature Key dialog box before using Switch Binding features. |
| Send firmware failed. | A firmware download operation failed. | Retry the firmware download operation. If the problem persists, contact the next level of support. |
| SNMP trap address not defined. | If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined. | Enter a corresponding SNMP trap recipient address. |
| Stop diagnostics failed. The test is already running. | Diagnostics for the port was not running and **Stop** was selected on the Port Diagnostics dialog box. Diagnostics quit for the port for some reason, but the **Stop** button remains enabled. | Verify port operation. Retry diagnostics for the port and select **Stop** from the dialog box. If problem persists, contact the next level of support. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| Stop diagnostics failed. The test was not running. | This action failed because the test was not running. | Informational message. |
| Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration. | The device WWNs were removed from the director's Switch Membership List (SANtegrity Binding feature), but you should note that one or more of these devices still has security control in port binding. | Verify that the security level for each device is as required by reviewing the Bound WWN list in the Configure Ports dialog box. |
| System diagnostics cannot run. The Operational Status is invalid. | System diagnostics cannot run on switches with failed ports | Replace failed ports. |
| Switch clock alert mode must be cleared before enabling period synchronization. | Clock alert mode is enabled through the Configure FICON Management Server dialog box and user is attempting to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box. | Disable clock alert mode through the Configure FICON Management Server dialog box. |
| The add firmware process has been aborted. | You aborted the process to add a firmware version to the HAFM appliance's firmware library. | Verify the firmware addition is to be aborted, then click **OK** to continue. |
| The data collection process failed. | An error occurred while performing the data collection procedure. | Try the data collection procedure again. If the problem persists, contact the next level of support. |
| The data collection process has been aborted. | You aborted the data collection procedure. | Verify the data collection procedure is to be aborted, then click **OK** to continue. |
| The default zone must be disabled to configure. | The message appears when you attempted to change the management style to Open Fabric and the default zone is enabled. | Disable the default zone and repeat the operation. |
| The Ethernet link dropped. | The Ethernet connection between the HAFM appliance and the director is down or unavailable. | Establish and verify the network connection. |
| The firmware file is corrupted. | A firmware version file is corrupt. | Contact the next level of support to report the problem. |
| The firmware version already exists. | This firmware version already exists in HAFM appliance's firmware library. | Informational message only—no action is required. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCNs. | You attempted to disable these parameters in the Configure Switch Parameters dialog box while Enterprise Fabric Mode is enabled. | Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in HAFM, then disable the parameters. |
| The link to the director is not available. | The Ethernet connection between the HAFM appliance and the director is down or unavailable. | Establish and verify the network connection. |
| The link to the switch is not available. | The Ethernet connection between the HAFM appliance and the switch is down or unavailable. | Establish and verify the network connection. |
| The IPL configuration cannot be deleted. | Deletion of the IPL address configuration was attempted and was not allowed. | Cancel the operation. |
| The management server is busy processing a request from another Element Manager. | The HAFM appliance is processing a request from another instance of an Element Manager, and cannot perform the requested operation. | Wait until the process is completes, then perform the operation again. |
| The optical transceiver is not installed. | Information is not available for a port without an optical transceiver installed. | Install an SFP optical transceiver in the port. |
| The switch did not accept the request. | The director or switch cannot perform the requested action. | Retry the operation. If the condition persists, contact the next level of support. |
| The maximum number of address configurations has been reached. | The maximum number of saved address configurations has been reached. | Delete configurations no longer needed to allow new configuration to be saved. |
| The switch did not respond in the time allowed. | While waiting to perform a requested action, the director or switch timed out. | Retry the operation. If the condition persists, contact the next level of support. |
| The switch is busy saving maintenance information. | The director or switch cannot perform the requested action because it is busy saving maintenance information. | Retry the operation later. If the condition persists, contact the next level of support. |
| The switch must be offline to change the Management Style. | The firmware is below the required level and you attempted to change the management style. | Select **Set Online State** from the Maintenance menu and click **Set Offline**. Then change the management style. Set the director or switch back online when finished. |

**Table 8** Element Manager messages (continued)

| Message | Description | Action |
|---|---|---|
| The switch must be offline to configure. | A configuration changed was attempted for a configuration requiring offline changes. | Take the appropriate actions to set the director or switch offline before attempting the configuration change. |
| This feature is not installed. Please contact your sales representative. | This feature has not been installed. | Contact your sales representative. |
| This feature key does not include all of the features currently installed and cannot be activated while the switch is online. | The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set, however, will remove current features not in the new feature set. | Set the switch offline through the Set Online State dialog box, then activate the new feature key using the Configure Feature Key dialog box.<br>The new feature key will display both the new features and the features that were installed previously. |
| This feature key does not include all of the features currently installed. Do you want to continue with feature key activation? | The feature set currently installed for this system contains features that are not being installed with the new feature key. | Click **Yes** to activate the feature key and remove current features not in the new feature set or **No** to cancel. |
| Threshold alerts are not supported on firmware earlier than 01.03.00. | Threshold alerts are not supported on firmware earlier than 01.03.00. | Informational message. |
| Unable to change incompatible firmware release. | You tried to download a firmware release that is not compatible with the current product configuration. | Refer to the product release notes or contact the next level of support to report the problem. |
| Unable to save data collection file to destination. | The HAFM appliance could not save the data collection file to the specified location (PC hard drive, CD, or network). | Retry the operation. If the condition persists, contact the next level of support. |
| You do not have rights to perform this action. | Configured user rights do not allow this operation to be performed. | Verify user rights with the customer's network administrator and change as required. |

# Index

## D



## E

## F



## H

## I



## K



## L

## M



## N



## O



## P

## R



## S

## T



## U



## V



## W



## Z